SECURITY MANAGEMENT

Preventing Workplace Violence

This collection of articles from the security profession's premier publication examines techniques and strategies security leaders can use to mitigate the risk of workplace violence.

SECURITY MANAGEMENT

Building a Hostility-Free Workplace

Positive and inclusive workplaces do not happen overnight. They are developed and sustained though training, teambuilding, education, resiliency, and sound policies.

By Raquella Solon

This is the #MeToo era. The great wave of public accusations involving inappropriate conduct such as sexual harassment between managers, employees, and coworkers has washed over U.S. workplaces, unsettling everything in its wake.

But sexual harassment is not the only conduct that can help turn a working environment hostile. Given this, employers and security managers who take action now to help establish and solidify a welcoming and hostility-free work environment will be better positioned for the future. Such actions can come in many forms, ranging from zero-tolerance anti-harassment policies and violence prevention training to diversity task forces and team-building exercises.

But while they vary, these actions all benefit from a proactive approach. Opposing views and opinions are inevitable among a diverse workforce, but leaders of organizations should not wait until disruptive incidents

break out before focusing on the state of the workplace environment. Instead, they can start immediately.

RESPECT AND DIGNITY

Security is a team sport. No one security director or manager, no matter how talented or knowledgeable, can completely shoulder the burden of protecting his or her firm. A cohesive security team, on the other hand, is positioned to tackle anything thrown its way. But when one gear gets out of whack, the whole team is affected and compromised.

Take, for example, one security director who we'll call Sam. The team was led by a small group of managers who worked well together; they collaborated to achieve goals and boost one another to success. However, a new manager, Chris, was brought on.

Chris has a markedly different type of attitude and leadership style. Chris is demanding, and sometimes even yells at employees in public. He occasionally disparages another manager's directions to team members and will go so far as to threaten a firing in an attempt to improve performance.

A few months after this leadership transition, some employees began to leave Sam's team by choice. But those are not the only changes triggered by the new manager. Some of Sam's team members have absorbed the negative qualities Chris exhibits, including degrading public chastisements, gossiping, and expressing increased agitation in the office. Chris' overwhelming negativity threw a wrench into a once strong security team and threatened to break it down into an unproductive group of individuals. Before Chris took over, Sam's team members respected one another and successfully accomplished goals. Chris' harsh leadership eroded the members' respect and kindness, causing productivity to decrease and spirits to drop.

How can this situation be avoided? When building a team, it is important to establish respect, dignity, and kindness as foundational principles. This will very likely increase productivity and reduce the risk of violent workplace behaviors. When employees feel respected and treated with dignity, they are more likely to treat coworkers and customers the same way. This creates a positive culture within the organization.

To facilitate this, security managers should go beyond simply asking employees to be civil and respect one another. They should also explain how to do so, and demonstrate what civility means to the organization by providing examples of positive interactions.

During my time as an assets protection manager, there were key opportunities for me to support the company culture. Security managers can take advantage of the same opportunities, if their organizations are willing to provide them.

For example, orientation sessions are an opportunity to introduce yourself, your department, and the values of the organization to those who are being onboarded. Time can be devoted to explaining appropriate workplace behavior through the use of scenario-based situations.

In addition, team meetings—whether daily, weekly, or monthly—offer opportunities for managers to touch on relevant issues and provide training through small group discussion or case study review. Individuals can assess a situation and provide feedback on how it should have been appropriately handled. Using both positive and negative behaviors for examples will help employees understand the difference.

Open houses are another possible venue for educating discussions. The security company may arrange with company leaders to have a time where employees come

in, ask questions, and participate in discussions that help workers understand their role as part of the larger effort to maintain a healthy workplace.

Finally, it is important to remember that security managers and staff should always be role models of appropriate behavior. If they are behaving badly by being rude, disrespectful, or uncivil, how can they expect to help the organization promote a culture that values everyone?

Orientation sessions are an opportunity to introduce yourself, your department, and the values of the organization to those who are being onboarded.

In the end, managers cannot assume that people understand what is and is not appropriate. Setting expectations from the start, and clearly demonstrating how to positively act and show respect to coworkers, is an effective way for managers to set the right tone—and a more active and effective approach than simply hoping for the best. This will have a ripple effect throughout the workforce, and it will help prevent future breaches of conduct from triggering a domino effect of disrespect, such as the one caused by Chris' behavior.

VIOLENCE PREVENTION

Another common violation of positive foundational workplace principles is workplace bullying. The following scenario illustrates some gender issues, which are starting to become more common in workplaces.

Stephen, a security department employee, was encouraged by ongoing legislation for gender-neutral bathrooms. As a result, Stephen approached a manager to explain that she gender-identified as female and would like to be referred to as Shawna. Shawna was later confronted by a handful of coworkers who said they would never support legislation

and would monitor the bathrooms should such laws pass. The confrontation caused Shawna to feel unsafe at work and scared to "come out" as a female to the rest of the office.

Depending on where Shawna lives, she may be protected. Approximately 20 states and 200 cities have laws that protect transgender individuals from discrimination specifically related to job status and/or promotion. However, just like bullying of a non-transgender person, there are limited laws preventing bullying types of behavior.

A key component to preventing bullying in the workplace is to start by defining what bullying is. Bullying involves repeated unreasonable actions with the intent to intimidate, degrade, or humiliate another individual or group of individuals. This can occur between any two coworkers or groups of coworkers, regardless of rank or status.

Hostile environments often stem from bullying, sexual harassment, or discriminatory conduct that interferes with an employee's ability to perform his or her job. In such environments, verbal, physical, or visual behaviors create an intimidating, offensive, threatening, or humiliating workplace. It's important to note that hostile behaviors can be perpetrated by anyone in the work environment, from employees to customers to vendors.

These situations can adversely affect an employee's psychological wellbeing. Moreover, the psychological injury that results from harmful conduct can be considered a form of workplace violence. Complicating matters is the fact that every employee brings a unique set of values, upbringing, experiences, and education into the workplace. Certain incidents, conversations, or remarks that may be acceptable to one may be harmful and injurious to another.

Luckily, various preventative measures are available to managers. Engaging in conversations about appropriate workplace behaviors helps to set a line between right and

wrong, so HR sessions that allow for this can be helpful. Gaining an understanding of what is and isn't considered harassment, bullying, and incivility allows employees to differentiate between certain behaviors and comprehend the context of any policies and procedures. Given the global diversity of most workforces, it is important to define and discuss what civility and respect mean to your organization to ensure everyone is on the same page.

Security managers also can implement violence prevention training. Just as it is vital to teach what behaviors are acceptable, it is a good idea to define and train employees on behaviors that are unacceptable through examples, case studies, or role playing. Setting a definitive line between right and wrong helps employees recognize these behaviors in themselves and others, mitigating the risk of conflict.

In the case of Shawna, the security manager eventually worked with HR to organize violence prevention training sessions for all employees. The sessions instructed employees about how to take steps in certain workplace situations. Furthermore, they allowed employees across the office to learn more about their coworkers and gain a better understanding of everyone's unique backgrounds and values. This strengthened respect for each other. Overall, the sessions were a success. Had they been implemented as a matter of course, they may have prevented the incident from ever occurring.

MULTI-GENERATIONAL TEAMS

Multi-generational workforces are here to stay. The members of Generation Z, or those born between the mid-1990s to the mid-2000s, have started to enter the workforce. They join the Generations Y (commonly known as Millennials) and X, and the Baby Boomers. In some workplaces, members of the Silent Generation are still productive in their seventies.

This age-diverse workforce can make for a rich and vibrant mix of ideas, opinions, and viewpoints. It also can cause problems when conflicts arise, and two employees don't see eye to eye. Given this, more employers are trying to keep up with changing demographics and are taking a closer look at office dynamics and making adjustments to fit their multi-generational teams.

To help create an environment where a diverse community of workers can collaborate, employers may create a multi-generational task force to survey their current workforce and gain a sense of what is useful and what is outdated. The task force should include at least two individuals from each generation represented in the workplace, with additional gender and cultural considerations applied. It may operate as an Employee Engagement Committee, with task force members serving as the voice of their fellow employees and implementing various staff celebrations. Members may also facilitate professional growth opportunities that appeal to the group of employees they are representing.

Another way to improve relations between generations is implementing an onboarding buddy system. New employees are paired with someone outside their own generation, allowing for an opportunity to learn while appreciating another's perspective.

Take, for example, a task force which includes members Kelsey and Carol, two employees who are nearly 30 years apart in age. As a Millennial, Kelsey prefers to receive information electronically through either text or email. She also prefers a manager who takes an educational approach and who takes time to understand her personal and professional goals. Like many Millennials, Kelsey also values meaningful work and desires to contribute to the larger mission.

Carol, a Baby Boomer, prefers face-to-face communication. She benefits from managers who take a democratic band-of-equals approach to working with a group, and who clearly define the team's mission. Carol is a dedicated worker and at a point in her career where she isn't really interested in moving ahead. She is counting down the days to retirement. She is willing to train her younger coworkers to step up and take on leadership roles.

Gaining a greater understanding of employees' management needs will help security managers create a more inclusive environment. Once organizations gain a better understanding of who their employees are as individuals, they can strategically partner with people who will work well together. The employer may realize Kelsey's strengths as a Millennial can be enhanced with a little coaching from a seasoned worker like Carol. Many Millennials grew up with a coach or mentor teacher who provided a positive influence, and they desire a similar relationship in their jobs.

Gaining a greater understanding of employees' management needs will help security managers create a more inclusive environment.

By pairing Kelsey with Carol in a buddy system, both stand to learn from each other. Perhaps Kelsey learns the inside scoop of the job while teaching Carol about the latest technology trends. This pairing helps coworkers relate to one another, create new bonds, and build new skill sets. Additionally, the teamwork between a Millennial and Baby Boomer prepares both employees as the Baby Boomer transitions to retirement. Carol can effectively

train Kelsey on her roles in the company so that when she retires, Kelsey is able to seamlessly take on new responsibilities without Carol's guidance.

One of the best things security managers can do to create connections between employees is to promote team development activities and implement cultural diversity training. Multi-generational workforces can learn about their younger or older peers through non-threatening teambuilding activities. Older employees' fears of feeling outdated may be lessened, and younger employees' frustration about being excluded from certain operations due to inexperience may be reduced.

These activities foster engagement between coworkers, allowing them to discover commonalities, as well as highlight what makes them valuable to the organization. They also make for a more comfortable workplace, and they foster the guiding principles of respect and inclusion.

IMPROVING WORKPLACE RESILIENCY

Resilience has recently become an important concept in many different arenas; cities, communities, and even countries are all striving to achieve it in different ways. It is also critical for a security team to exemplify resiliency. In this case, resiliency describes the capacity of people, organizations, or systems to adapt to changing conditions and rapidly recover from disruption.

To improve the resiliency of a security team, it is advisable to incorporate overall concepts of resilience into existing training programs. For example, a shared understanding of the roles and responsibilities of team members can greatly reduce the stress on the team and therefore increase resiliency. Moreover, each individual employee has an innate level of resilience that can be further developed through training.

Just as training employees helps to build confidence, so does recognition of performance. Thus, one of the most direct ways to increase resiliency is to build people up by recognizing them for their work. The act of thanking employees and acknowledging quality work helps create a positive and productive environment—in effect, the opposite of a hostile workplace. When people feel appreciated, they often feel more energetic, and are willing to go the extra mile when the going gets tough.

I used to work as an operations manager of a retail store. I realized the importance of maintaining resilience and of expressing my appreciation for my staff's hard work. Therefore, I would look for ways to show them my appreciation. After an especially challenging week, I called a team meeting to recognize everyone's hard work and thank them for their dedication. I showed them my gratitude with a catered meal accompanied by praise and motivating remarks for continued success.

In addition to showing appreciation, managers can also offer rewards for exceptional work. For example, I implemented a "recognition wall" that encouraged employees to fill out a card briefly detailing something another employee did and add it to the wall. The actions written about could be as simple as someone going out of his or her way to help a fellow coworker or customer. In a seemingly small but important way, the system allowed employees to support one another, boost each other's confidence, and ultimately enhance company morale.

I also required my leadership team to write out three to five cards per shift to keep the wall filled with positivity each day. Within three months, the culture of the workplace improved dramatically; many employees who had been disheartened and unmotivated became much more engaged. The employee attrition rate also dropped from 30 percent to 20 percent.

A workplace where employees do not feel valued or recognized is not a positive workplace. Often, it is one where employees feel they need to escape; they feel that management is not helping them feel like a part of a mentally and emotionally safe and healthy environment. This in and of itself may not constitute a hostile environment, but it is likely close to one.

USING AN EAP

Security work can be highly stressful, and stressful work situations can lead to anger, withdrawal, and even situations of workplace violence. Stress, anxiety, and depression do not just affect the employee suffering from them. The employer and the company are also affected, by way of factors like lost production time and negative effects on coworkers.

To help prevent violence between stressed coworkers, HR and managers should take note of signs and symptoms of stress and attempt to address changes in behaviors. Behaviors to look for include decreased productivity, frequently arriving to work late, and sudden shifts in mood.

According to the U.S. Bureau of Labor Statistics, there were 866 fatal work injuries involving violence in 2016. To keep employees safe, security managers can train all employees to recognize warning signs of workplace violence. Training should include steps to take for violence prevention and verbal intervention. Security managers also should encourage employees to notify them of any threats, so they're able to take action before an incident occurs.

Additionally, employers can provide an employee assistance program (EAP) in their employee benefits package. An EAP provides quick, reliable guidance on everything from stress management to family care options so staff can come to work with greater peace of mind. A good EAP helps

alleviate stress and worry, connects employees with the resources they need to manage their mental health, and helps prevent potential violence before it occurs.

Take the example of Patrick and Jordan. Patrick is a long-term employee struggling at work due to personal dilemmas stemming from a rough divorce. Jordan, Patrick's manager, noticed a marked decrease in Patrick's productivity and engagement. Jordan took Patrick aside to discuss the productivity problem. When Patrick shared his personal struggle, Jordan was able to provide resources to help Patrick via the company-provided EAP. The EAP offered guidance and a referral to a local counseling professional. With this support, Patrick was able to adjust to the changes taking place in his life and return to work with a greater sense of normalcy.

Of course, a solution like this one is not always possible in every case. Many employers do not provide an EAP; if they do, employees are unaware it is available or believe it isn't confidential. Inattentive managers or fellow coworkers may not notice the warning signs, and the stressed employee will keep his or her feelings bottled up. When this is the case, the employee can lose control and become verbally or physically violent towards coworkers. With the appropriate training and resources, all members of a security team are able to de-escalate and curtail potentially troubling situations without resorting to physical confrontation.

COMPANY POLICIES

The workplace should be an inclusive environment where employees feel safe to effectively share ideas and join forces to create new ones. Going the extra mile to develop a welcoming community for employees will help security teams thrive and improve the likelihood that the work pro-

duced there will be exceptional. Moreover, it is the responsibility of managers to create and enforce the policies and procedures that will guide employees towards resilience.

Establishing specific and explicit policies regarding harassment, bullying, and violence, which also include plans and procedures for responding to incidents, is essential. These response plans should include processes for communicating with employees, families, and the media, working with law enforcement, and a capacity for staff debriefing if any type of violence is committed, threatened, or observed. As part of the onboarding process, new hires should be made aware of the plan, so they are well-versed on the organization's policies.

With these policies in place, the next step is to consider using some of the training programs mentioned above that will develop employees as team players, improve overall productivity, and mitigate problematic workplace behaviors. Finally, security managers should continuously review how employees interact with one another and update policies and procedures to fit the needs of their advancing workforce.

RAQUELLE SOLON IS A BUSINESS SOLUTIONS ENGINEER FOR FEI BEHAVIORAL HEALTH IN MILWAUKEE, WISCONSIN. SHE IS RESPONSIBLE FOR, AMONG OTHER THINGS, HELPING ORGANIZATIONS IMPLEMENT CRISIS MANAGEMENT SYSTEMS AND WORKPLACE VIOLENCE PREVENTION STRATEGIES. SHE WAS NAMED "WOMAN OF THE YEAR" FOR 2012-2013 BY THE NATIONAL ASSOCIATION OF PROFESSIONAL WOMEN.

SECURITY MANAGEMENT

An Intelligent Solution

As concerns about workplace violence rise, companies should adopt protective intelligence strategies to prevent attackers from succeeding.

By Cody Mulla, CPP

A large, international finance company was recently planning to fire one of its employees, but the company's leadership was concerned. The employee, whom we'll call John, had a history of being aggressive towards his supervisors.

Thankfully, the actual termination went smoothly and without incident, but that's where the company's good fortune ended. During the days that followed John's termination, several employees received notes from him on social media instructing them to "consider not going to work" on a specified day.

As a precautionary measure, the company contracted for additional physical security at its main office building. However, when it became aware of the social media threats, the company reached out to the author's international protection, investigations, and consulting firm for advice on how to handle this new challenge.

The firm immediately began conducting physical surveil-

lance, following John's movements. It also started analyzing his social media accounts and noticed that he had made several posts about the company's vice president of human resources.

Upon further observation, the firm discovered that John had recently driven to an intersection about one mile from the company's building. This location was also on the route that the vice president took to get to work every day.

Using the intelligence gathered from social media and physical surveillance, the firm observed John's behavior in real time and contacted law enforcement to prevent him from causing any harm to the vice president or to the company's facility.

Not all workplace violence threats are so successfully mitigated. An average of 551 workers were killed each year between 2006 and 2010 as a result of work-related homicides, according to the most recent numbers from the U.S. Bureau of Labor Statistics (BLS). And as many as 2 million workers report having experienced workplace violence each year, according to the Census of Fatal Occupational Injuries.

Most alarmingly, shootings accounted for 78 percent of all workplace homicides—83 percent of which occurred within the private sector.

Unfortunately, the traditional corporate climate is reactive because most companies only respond after there's been a highly publicized workplace violence incident. Furthermore, many do not enact changes at all once the dust settles and the incident is no longer in the media.

With concern growing over workplace violence from all sectors, there is a demand for protective intelligence, which can avert a crisis instead of reacting after it occurs.

To put it simply, you cannot mitigate a risk that you have not anticipated.

INTELLIGENCE

The primary objective of protective intelligence is to collect information to help determine if an individual demonstrates the intent and capability to formulate and execute a violent plan of action.

To determine this, most use the intelligence cycle—an important process for investigators or anyone who collects information for assessment or analysis.

Originally implemented by the U.S. Military Intelligence Division during World War I, this process is leveraged by many government entities and for a wide spectrum of tasks, such as by organizations like the Federation of American Scientists. This process is most notably used in the investi-

Protective intelligence investigations are performed most effectively by those who have experience and training doing them.

gative processes within the FBI and within the U.S. Secret Service, namely the National Threat Assessment Center.

The FBI defines the intelligence cycle as "the process of developing unrefined data into polished intelligence for the use of policymakers." Protective intelligence investigations differ from other kinds of investigations because the goal is to prevent violence or a loss, not simply secure the requested facts.

An individual, group, or organization must collect information that will develop the critical intelligence required to take preventative actions. The U.S. Secret Service defines this process as "gathering and assessing

information about persons who may have the interest, motive, intention, and capability of mounting attacks against public officials and figures."

The intelligence cycle has six steps. These steps are: identify requirements, plan and provide direction for intelligence that is to come, collect and gather information, process and exploit collected information, analyze and convert that information to produce raw intelligence, and disseminate intelligence to those who will use it for tactical, operational, and strategic decision making.

Identify requirements. The first step is to identify the requirements the information is designed to satisfy. This step will help filter data into the most critical pieces of information and organize them by relevance.

For workplace violence investigations, investigators should focus on information that will help answer the fundamental question: Does this subject present a threat to protected individuals, groups, or organizations?

Some companies do designate internal employees as threat response personnel. Protective intelligence investigations are performed most effectively by those who have experience and training doing them and who are also unbiased, such as a third-party consultant.

Plan and provide direction. The second step in the cycle is to create a plan and provide direction for the intelligence that is to come.

Collect and gather information. Gathering of information is the third step and includes researching online databases, performing physical surveillance, and conducting interviews.

Process and exploit. After collecting relevant information, the fourth step of the intelligence cycle is to process and exploit that information. This means filtering the data into useable bits for the decision-making processes

defined by the requirements in the first step; the bits can be referred to as the dots.

For example, when conducting an investigation of a subject who may be on the path to violence, social media or other tools may reveal his whereabouts during certain times that may be indicative of a hostile planning process. Critical decision points for likely pathways the subject would take to commit an act of violence could be established, and their correlation with the information

"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."

that has been revealed would create the dots.

This can be a time-consuming burden, especially for investigators using social open-source intelligence (SOSINT). To be effective at this task, investigators should combine resources by directly researching on social media sites and by using search engines to do the task. With this methodology, investigators can start to connect the dots, enabling analytical confidence—particularly when dealing with the concern of targeted violence.

Analyze and convert. The fifth step of the process is to analyze and convert these bits of data to produce raw intelligence.

In the event that a subject's behavior reveals the impending manifestation of a perceived threat, these connected dots are used to make decisions that will effectively impede the process.

Disseminate. The final step of the cycle is disseminating

the intelligence to those who will use it for tactical, operational, or strategic decision making.

SOURCES

Although most would believe that intelligence is gathered from secret or covert sources, the largest collection of information available to investigators is open-source intelligence (OSINT), or intelligence collected from publicly available resources.

Within the intelligence community, the term "open" refers to overt, publicly available sources drawn from public resources, such as the Internet, media coverage, photos, and geospatial information. However, it's important to keep in mind that there is no authority ensuring the accuracy of any information available through OSINT. Because of this, employers who use this collection method have a responsibility to verify—or at least corroborate—its validity.

SOSINT, the collective term for information from sources such as Facebook, Twitter, blogs, and microblogging sites, is becoming more important within the intelligence community. SOSINT is a content-rich gold mine and a valuable investigative tool when seeking corroborative information about individuals or groups, such as behavioral changes, interests, emulations, gang activity, and general life circumstances.

Social media is particularly useful to investigators for several reasons. The first is the immediacy in which content is not only created, but disseminated. The Facebook news feed is the epitome of a media outlet for such content because there is no delay in publication and almost no restriction in its ability to spread virally. Social media provides a variety of ways for potential subjects to distribute thoughts or request tactical assistance,

along with numerous ways for investigators to gather that information.

In 2014, LexisNexis published a survey, Social Media Use in Law Enforcement, of federal, state, and local law enforcement professionals in the United States who are users of social media on the job. The survey details how social media can enhance the assessment and threat management process.

The survey found that "respondents indicated several real-world examples in which they prevented or thwarted pending crime, including stopping an active shooter, mitigating threats toward school students, executing outstanding arrest warrants, and actively tracking gang behavior."

For the private investigator seeking information on the behavioral circumstances of a subject, something as quick and easy as analyzing a subject's status updates, check-ins, and posted photos may provide the information necessary to conclude if a legitimate threat exists.

SURVEILLANCE

Physical surveillance is one of the oldest and most common practices within investigative services, yet it remains the best option in cases when real-time information is required. To do this, employers must hire a licensed professional who can conduct surveillance legally.

Surveillance in the investigative field is used mostly as a tool for developing factual evidence to prove or disprove circumstance. However, surveillance can also provide information that is critical to the decision-making process for a much broader spectrum of investigations than most private detectives recognize.

In conducting protective intelligence investigations, surveillance is a viable option to gather the necessary information on a subject because not all attackers make

direct threats. This increases the difficulty of validating or legitimizing the threat through other sources.

Using information from OSINT may reveal the threat, such as general ideas and interests, but it is typically not specific. Surveillance can be used to confirm a suspected threat or to find out more details.

Furthermore, the analytical confidence from deriving conclusions based on direct observations versus assessing the quality and quantity of third-party information is an important factor. This provides the investigator and analyst a more profound confidence in the facts at hand.

"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."

In one such instance, upon investigating a subject who was facing possible termination following a history of unsatisfactory performance and increasingly aggressive behavior, the author's firm noted a hunting license in the subject's background investigation.

Taken in isolation, this is not a threatening piece of information. However, during the day of a contentious announcement of the firing from the company's CEO, it was decided by the author's firm—hired to provide executive protection for the company—to restrict access to the facility.

Local law enforcement helped bar the subject from the property. The former employee had a hunting rifle in his vehicle even though no hunting seasons were in effect. There was no violence that day, but the potential mitigation was worth the effort.

Once the subject is identified and background information has been collected, the main factors investiga-

tors should concentrate on during surveillance are the current living characteristics of the subject and context of the subject's daily routine.

Surveillance should focus on factors in the subject's life and environment that might increase the probability of an outburst or attack, such as living arrangements; actions and behavior; and daily activities and social interactions, particularly compared to possible known historical circumstances and behavior of the subject. This focus on routine can provide valuable information that can help assess the subject's stability.

For example, if the subject does not currently have the means to satisfy the basic needs of food, clothing, shelter, or social interaction, then he or she may be in desperate crisis with no option left but to act out.

Additionally, researching, planning, and coordinating the attack are critical to the attacker's success. The steps required in developing a plan will reveal the person's intentions, actions, and acquaintances.

For instance, this can be seen in the events that led up to the kidnapping of Sidney Reso, former president of Exxon Co. Reso was kidnapped by Irene Seale and her husband Arthur Seale from the end of Reso's driveway in suburban New Jersey on April 29, 1992. Reso was shot in the arm during the kidnapping, and died a few days later. However, the Seales claimed that he was alive and demanded $18.5 million in ransom before finally being discovered and apprehended.

Prior to kidnapping Reso, the Seales watched his home from a van parked down the street for almost a month. These preparations were highly visible and could have been easily identified. The Seales could have potentially been intercepted with a counter surveillance effort as part of an executive protection program.

For violent attackers, the chances of success and escape are the predominant factors in determining the location to attack. Therefore, research and planning efforts on site selection and even tactical decisions pertaining to that site are particularly revealing during physical surveillance. The subject's behavior and rituals during this process are also extremely revealing because the attacker's intention may not include any escape plans at all, potentially indicating the worst case scenario of a suicide attack.

This type of behavior was demonstrated by Khalid al-Mihdhar and Nawaf al-Hazmi who flunked their flying lessons because they were disinterested in the landing process, administrative actions, or flying anything other than Boeing jets. The two individuals failed to obtain their pilot's license, but ended up being two of the four "muscle men" on American Airlines Flight 77, which flew into the Pentagon on 9/11.

The potential attacker will want to gain familiarity with the location, how to get there, and—in most cases—how to escape. He or she may even take pictures of the location for reference later in the planning process, and may conduct rehearsals to discover what the security response might be during a crisis or how effective access control is.

In the investigation that followed the mass shooting in the Aurora, Colorado, movie theater, it was revealed that gunman James Holmes had purchased his ticket for that showing of The Dark Knight Rises more than a week in advance, carefully selecting the time and place for his attack.

Additionally, he had set explosive traps at his apartment, planning for them to be tripped prior to his attack to send resources to that incident instead of the movie theater.

Real-time information gathered via surveillance can lead to making preventative decisions sooner and more reliably than other methods of investigation.

Examples of behaviors that may indicate the coordination or planning of an attack could be visiting others who share the same ideas and interests, visiting websites linked to the company, obtaining supplies, or purchasing weapons. At this point, the investigator should avoid bias and assumption, concentrating only on facts.

For example, if a suspect who has no historical interest in firearms obtains weapons and ammunition over the course of an investigation and then proceeds to a target location, investigators conducting the surveillance may be able to involve the authorities immediately.

To be effective at surveillance, the investigators must anticipate the subject's actions. Investigators must ask themselves where the subject would have to be and what materials would have to be obtained. To that end, investigators should develop a list of locations and activities that may be part of the subject's target selection or planning processes.

For investigators, protectors, and those who conduct threat assessments and evaluations, protective intelligence programs are a critical aspect of proactively preventing workplace violence incidents before they occur. When it comes to reducing workplace violence as a whole, we all share the responsibility of identifying, assessing, and intervening as early as possible.

JOSEPH M. LASORSA, CPP, IS SENIOR PARTNER AT LASORSA & ASSOCIATES, AN INTERNATIONAL PROTECTION, INVESTIGATIONS, AND CONSULTING FIRM. HE MANAGES AND CONDUCTS PROTECTIVE OPERATIONS TRAINING COURSES AND SPECIALIZES IN EXECUTIVE AND BODYGUARD SERVICES; RISK MANAGEMENT CONSULTATIONS AND SEMINARS; WORKPLACE VIOLENCE PREVENTION SEMINARS AND INTERVENTION SERVICES; SECURITY CONSULTATIONS AND SEMINARS; PRIVATE INVESTIGATIONS; AND TECHNICAL SURVEILLANCE COUNTERMEASURES.

SECURITY MANAGEMENT

Guidance on Threat Assessment Teams

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 Cody Mulla, CPP

Recent guidance from the U.S. Secret Service, Enhancing School Safety Using a Threat Assessment Model: An Operational Guide for Preventing Targeted School Violence, offers baseline information for developing a threat assessment team (TAT) to mitigate potentially violent or devastating events at K-12 schools in the United States.

The Secret Service advocates for a five-step process to establish a TAT with a multidisciplinary approach to information sharing. For each step, the author will provide guidance that extends beyond the scope of the Secret Service report with additional threat prevention measures.

1. ESTABLISH A MULTIDISCIPLINARY TEAM.

The TAT is designed to direct, manage, and document threat assessment processes. Assemble a team from a variety of disciplines, which may include teachers, school

guidance counselors, coaches, school resource officers, mental health professionals, and school administrators. Have a designated leader with the authority to act immediately in cases where time is of the essence. Meet on a regular basis and when needed if there is an emergent concern. These meetings should include dealing with potential threat indicators, training and role-playing focused on building confidence and capability, and building rapport and confidence in other team members.

Additional guidance: Threat assessment is an intelligence-led activity and requires a certain skill set to synthesize information. Schools could partner with an agency or consider employing an employee with an intelligence background. The Multi-State Information Sharing and Analysis Center (MS-ISAC) also offers valuable trend information on physical and cyber threats that could be useful for the TAT.

2. DEFINE PROHIBITED AND CONCERNING BEHAVIOR. Concerning behavior progresses through a continuum, and policies must consider warning signs, which include "a marked decline in performance; increased absenteeism; withdrawal or isolation; sudden or dramatic changes in behavior or appearance; drug or alcohol use; and erratic, depressive, and other emotional or mental health symptoms," according to the report. Policies and procedures should be set in place to monitor and direct action to collect additional information to consider if these are indeed a concern.

Additional guidance: The Secret Service does allude to a continuum, but there is no specific guidance on how to categorize threats. A more in-depth understanding of transient and substantive threats is needed. It may be advisable to develop a tailored process map for each TAT,

which describes each step and indicates responsibility in each phase to avoid anything falling through the cracks.

3. CREATE A CENTRAL REPORTING SYSTEM.

Establishing a central reporting system is crucial to all other threat assessment activities. Schools should establish multiple streams of information that could include online reporting, email, phone, and face-to-face communication. No reporting should be dissuaded but educating the school community on what to report will increase the validity of information. Document thoroughly when responding to each report, categorizing threats, and determining whether to act. Anonymous reporting should be an option for those who are uncomfortable coming forward in a formal or public way. It is important to handle each case with professionalism, considering privacy and confidentiality concerns.

Additional guidance: Consider partnering with an Information Sharing and Analysis Center (ISAC), which is a nonprofit organization that provides an avenue for two-way sharing between the public and private sectors. Though ISACs have traditionally dealt with cyber and physical security, the model could be used to develop information sharing practices related to threat assessment.

4. DETERMINING THE THRESHOLD FOR LAW ENFORCEMENT INTERVENTION.

Law enforcement intervention may be needed in some cases, though it may not be involved in all threat assessment efforts. Create policies and procedures to indicate when law enforcement should be involved—for example, in cases that deal with weapons, threats of violence, and physical violence. Law enforcement should be involved when elements of a crime are present.

Additional guidance: Certain privacy laws set limitations on law enforcement activity when it comes to minors. School

administrators and the TAT should familiarize themselves with state law before developing policies and procedures around law enforcement response.

5. ESTABLISH ASSESSMENT PROCEDURES.

Establishing threat assessment procedures will help paint an accurate picture of the student's thinking and behavior, formalize a reporting structure, and identify appropriate interventions. Documentation is once again stressed, with creation of forms and templates to capture necessary information. The report recommends a community-wide approach and encourages a brainstorming exercise on sources of potentially helpful information. This exercise can be repeated once an individual of concern is identified for information more specific to that person. Additionally, social media should be examined to gain information, interviews should be conducted, and the student's locker should be searched.

Additional guidance: The Secret Service guidance seems to only consider internal threats—mainly students—but narrowing the focus is a risk in and of itself. A threat could be anyone: a teacher, contractor, administrator, or someone not associated with the school.

Threat assessment is a necessary part of threat prevention at every K-12 school. Threat assessment programs and teams will be more successful if they are a function of an overarching enterprise risk management process, fueled by both internal and external sources of information.

CODY MULLA, CPP, HAS 20 YEARS OF EXPERIENCE IN SECURITY AND CRISIS MANAGEMENT. HE HAS WORKED SUPPORTING BOTH THE PRIVATE AND PUBLIC SECTORS AND IS A MEMBER OF THE ASIS INTERNATIONAL SCHOOL SAFETY AND SECURITY AND COUNCIL AND THE UTILITIES SECURITY COUNCIL.

SECURITY MANAGEMENT

Culture Conflicts

New research into organizational culture traces workplace conflict back to six core elements that can tip an environment from healthy to toxic.

By Claire Meyer

Culture breeds conflict. According to the 2020 Workplace Culture Report from workplace education and analytics company Emtrain, workplace culture is how people interact and treat each other in the workplace, and elements of those cultures will influence whether the organization is a positive or toxic workplace.

"We have seen for many years now, as company stakeholders, we have to deal with these bad outcomes that seem to catch us by surprise," says Janine Yancey, CEO of Emtrain. "The idea was to take these bad outcomes—the tricky culture issues like harassment, bias, ethical mistakes, violence—and map them back to the indicators that are tied to behaviors or situations that, in heightened levels or when combined with each other, produce these bad outcomes."

The research from a database of responses from 40,000 employees across more than 125 companies traces workplace conflict back to six key indicators: three people indica-

tors (unconscious bias, social intelligence, and preexisting mind-sets) and three organizational indicators (in-groups and out-groups, power dynamics, and norms and practices).

"This is just part of being human—we carry our proclivities into the workplace," says Yancey. "It's the human condition, and when not well-understood and broken down into patterns we can all understand and process, then we're just going to be emotionally reacting off each other, and that's what breeds conflict."

That reactive stance can have serious consequences for organizational safety and security, says Steven Millwee, CPP, president and CEO for background screening and investigations firm SecurTest, Inc.

"A lot of misbehavior happens in organizations that have a toxic work environment; that's the sheer motivation for destruction of property, the theft of intellectual property, stealing, or just becoming abusive," Millwee says.

"If you work in an atmosphere where your manager is extremely toxic, you feel unappreciated, you feel isolated, no one listens to you, no one cares about you, your management team is totally disengaged from you," he adds. "This oppressive type of atmosphere motivates a person to not do their job—or just do the bare minimum of the job—or it creates a catalyst for the employee to act out because they feel they need to take some action, albeit inappropriate action. This can lead to all kinds of misbehavior as punishment for the way they are being treated. It doesn't justify their behavior, but it shows you the motivation that generated it."

Unconscious bias. As employers commit to diversity goals and workforces become more multicultural and multigenerational, these unintended, learned stereotypes come to the fore.

The Emtrain study found that more than half of employees surveyed report working with five or more diverse

coworkers of different races, genders, or generations in their teams, although they have yet to see that much diversity among executives.

In addition, although organizations increasingly encourage workers to voice their opinions and "bring their whole selves to work," the report said, only 32 percent of respondents said they strongly agree they can be their authentic self in the workplace.

On this factor, awareness is an essential first step. But awareness alone will not decrease the effect of unconscious biases. Most employees don't see the processes that organi-

Teaching healthy conflict resolution skills could make the difference between keeping and losing top talent.

zations can use to mitigate unconscious bias, such as role modeling, consistent employee evaluation, and equal division of support tasks.

Social intelligence. This is the ability to recognize and negotiate the social dynamics of the workplace, and these skills vary widely across the workforce. Only 46 percent of employees surveyed by Emtrain said their coworkers understand the impact their words or behaviors have on those around them, and just 23 percent said their coworkers can accurately pick up on the mood in a room.

The study found that 86 percent of employees strongly agreed empathy is important at work, but only 42 percent strongly agreed that they see it from their colleagues. The study also found that when employees experience lower levels of social intelligence from their colleagues, they also experience lower levels of trust and respect. In addition, employees are less likely to feel safe speaking up.

Preexisting mind-sets. "Employee expectations and

perceptions about what constitutes respectful behavior are informed by life experience," the report said. "As our workforce diversifies, employee perspectives will likely diversity as well."

Employees carry different perceptions of experiences and conflicts with them, and they often see their perspective as the correct one—amplifying the potential for conflict and misunderstanding. They bring similar diversity and preconceptions about how to resolve conflict. In a scenario where employees were asked how they would address a significant conflict between people with different life experiences, the majority (60 percent) would reengage their manager later to discuss what happened, but 26 percent would go to HR or a senior leader to discuss or complain, 7 percent would do nothing, and 7 percent would consider job hunting or changing teams at work.

"Teaching healthy conflict resolution skills could make the difference between keeping and losing top talent," the report said.

In-groups and out-groups. Most people can easily recognize in-groups from their school days: cliques, popular groups, the "it crowd." At work, these groups can form around race, gender, political beliefs, or other factors. People in out-groups receive less trust and support from their managers compared to members of in-groups. For example, 63 percent of in-group employees surveyed said that if they report something, they are confident management will take the complaint seriously. Only 40 percent of out-group employees said the same.

These groups also color how an employee's actions are perceived by their peers and coworkers. For example, when shown a video scene of harassing behavior, employees were less likely to classify the behavior as misconduct when the perpetrator is a person in power or a member of a perceived

in-group, Yancey says. Members of more marginalized out-groups were met with less empathy and compassion.

"This research proved out that certain demographics really do have second-class experience," Yancey says. While the separate treatment does not reach the level of a legally actionable different experience in the workplace, it's very subtle—and it adds up—she notes.

Power dynamics. The use of hierarchical power by managers can range from coercion to influence to empowerment. "The reason power dynamics are so important in understanding the health of workplace culture—where a manager has discretion over the daily activities, career progress, and livelihood of other employees—is that the consequences of employees' speaking up in an unhealthy situation can be so, well...consequential," the Emtrain report said.

While the majority of managers are not tyrants—most survey respondents said it is rare for people to get away with disrespectful behavior because of their authority—nearly one-third of survey participants identified power disparity as causing the greatest level of conflict at work. More common than tyrant managers are clueless managers. Only three in 10 employees said they are unlikely to say no to a boss's inappropriate request, but employees say only one in five managers understand that employees have a hard time refusing.

"The result: managers do not get the feedback they need when they misstep and employees tolerate disrespectful behaviors they would not accept from others," the report said.

Power dynamics can shift in a toxic direction, especially when combined with one or more of the personal cultural factors. If a manager has power but weak social intelligence skills, employees may feel uncomfortable or underappreciated, but could be unwilling to speak out for fear of repercussions.

Imbalanced power dynamics can also be expensive for the organization.

According to July 2019 research from the Society for Human Resource Management (SHRM), workers consider culture and managers to be closely connected. The report, The High Cost of a Toxic Workplace Culture: How Culture Impacts the Workforce—and the Bottom Line, found that 58 percent of American employees who quit a job due to workplace culture say their managers are the main reason they left. This turnover, SHRM reported, cost employers $223 billion over a five-year period.

Norms and practices. These are the spoken and unspoken rules that govern what is and is not appropriate workplace behavior. Deliberate, positive norms are the strongest predictor of healthy culture, and they can counterbalance negative effects from the other cultural indicators, the report said. Norms and practices are essentially a guide to "the way we do things here," the report said.

While the majority of managers are not tyrants—most survey respondents said it is rare for people to get away with disrespectful behavior because of their authority

---

"We all as humans have our own peccadillos—we all have our unconscious biases, our social intelligence is strong or not so strong, our preexisting mind-sets from our last job or experience. We bring all that with us into the workplace. The way to balance that out is having strong norms and practices," Yancey says.

However, only half of employees see strong norms and practices at their companies. Out of the 125 companies included in

the report, the healthiest organizations' employees said they were guided by strong norms and practices, Yancey notes. Among employees who see strong norms at their workplace, 75 percent said their organization is healthy, compared to 32 percent of employees who do not see strong norms.

Without strong norms, however, "it's a vacuum. Anyone's behavior can basically set the culture," she says. "You'll have a culture, it just won't be one that is intentional or proactively set. It's one that is created by usually the worst behaviors and worst elements of the organization."

Strong norms can be built in a variety of ways, including leaders' role modeling, training, skill building sessions, constructive feedback structures, and compelling change stories, the report said.

Security professionals can influence company culture by serving as eyes and ears within the organization and reporting on misconduct—even outside the security department, says Millwee. This helps to spread the burden of reporting outside a manager's direct reports, who may not feel comfortable coming forward.

Security practitioners can also understand where their organization's cultural hotspots are and serve as a cross-department collaborator to help address them, she says.

One rapidly emerging hotspot, especially in the United States, is politics, she adds. With a contentious election on the horizon and increasingly polarized political factions, workplaces could face heightened tensions. In addition, the coronavirus pandemic has thrown a wrench into many employees' long-term financial plans and ratcheted up health concerns. Altogether, these are ingredients for an explosive situation that could affect overall workplace culture as well as security, Yancey says.

However, "we're going into a rough business climate, both economically and civically, because of healthcare. Culture

can either really help be the rudder that steers the organization forward, or it's toxic, which means there's no rudder and the organization's spinning," Yancey says.

"On one positive note," Millwee says, "the challenges that employers are going through right now, just with the COVID-19 pandemic, really create an opportunity for a reset of where their cultures need to be refined."

"Employees working from home or not working at all may be very anxious or worried about what the future looks like. Sometimes we tend to minimize what others are thinking or feeling, but really their feelings and thoughts are just the same as ours," he adds. "By showing a sense of compassion and mercy—not shooting the walking wounded—you can engage your people and let them know that they can feel safe in your workplace. That can do more for your culture in today's situation than almost anything else."

SECURITY MANAGEMENT

Breaking the Silence

The more personal a problem is, the less willing people are to report it. But when domestic abuse threatens to escalate into workplace violence, early warning is essential.

By Claire Meyer

Dr. Tamara O'Neal called off her wedding. A few weeks later in November 2018, the emergency physician's ex-fiancé, Juan Lopez, confronted O'Neal at work at Chicago's Mercy Hospital and Medical Center. Lopez shot and killed O'Neal in the hospital parking lot, then proceeded to run inside the facility, firing at responding hospital police and employees. A Chicago police officer, a pharmaceutical assistant, O'Neal, and Lopez all died in the incident.

The separation of work and personal life has always been tenuous; employees take work home with them, and their personal challenges follow them to work every day. Sometimes these challenges are innocuous—an employee's child got a bad report card, and the employee is distracted thinking about it all day. But sometimes these challenges have more serious implications—an employee's ex-spouse has been making threatening calls to the organization, stalking her to work, and posing a security risk to the employee, her coworkers, and the organization.

In the past, "There was a real belief in the world of business that domestic violence was a personal matter," says James Cawood, CPP, PCI, PSP, president of Factor One, a threat assessment and management organization. "That was something that the individual had to deal with. There was no responsibility on the part of the business. And that was something that needed to evolve and change."

The upcoming new version of the ASIS Workplace Violence Prevention and Intervention standard includes domestic violence as a part of workplace violence mitigation strategies, says Cawood, who is a member of the ASIS working group revising the standard. By combining the two elements instead of marking intimate partner violence (IPV) out as a unique threat, security professionals can begin to break down taboos around discussing domestic abuse threats, he adds. However, there are still unique elements in responding to domestic abuse threats in a compassionate, mindful way.

"Domestic abuse is a little bit of a different creature, legally, than workplace violence in a robbery," says labor and employment lawyer James Curtis, a partner at Seyfarth Shaw. "There are different tools that employers should be thinking about and using to assist in their employees' situations." Curtis recommends making domestic abuse part of the organization's overall workplace violence prevention program and surveying employees to identify different areas that could pose significant hazards—unsecured entrances, unlit parking lots, and public-facing jobs that make access to employees easy.

In addition, organizations should provide a confidential conduit for employees to disclose concerns or abuse. "It's a very sensitive topic, and people are very reluctant to share that there is an issue," says Curtis. The organization can't help employees unless it knows about a problem. "So

you need to make sure there is a system in place to notify either HR, their supervisor, or a hotline so that they can do so confidentially with the comfort that they know it's not going to become the subject of workplace gossip," he continues.

A WIDESPREAD PROBLEM

The United Nations (UN) estimates that 35 percent of women worldwide have experienced either physical or sexual intimate partner violence or sexual violence by a non-partner, and some studies show that up to 70 percent of women have experienced intimate partner violence in their lifetime. In the majority of countries with available data, the UN reports, less than 50 percent of women who experience violence seek help; less than 10 percent seek help from law enforcement.

In the United States, more than 10 million women and men are physically abused by an intimate partner each year, according to the National Coalition Against Domestic Violence (NCADV). IPV encompasses physical violence, sexual violence, stalking, and psychological aggression perpetrated by a current or former spouse or dating partner. U.S. crime reports suggest that 16 percent of homicide victims are killed by an intimate partner.

On the job, 40 percent of women who died as a result of workplace violence in 2016 were killed by domestic partners or relatives, according to U.S. Department of Labor, Bureau of Labor Statistics (BLS). According to a 2006 study from BLS, nearly one in four large private industry organizations had reported at least one incident of domestic violence—including threats and assaults—in the previous year. A 2005 study of full-time American employees found that 44 percent had personally experienced domestic violence's effect in the workplace.

Domestic violence affects men as well; a 2018 study in the United Kingdom found that 9 percent of British men (1.4 million people) had experienced some form of partner abuse. A 2014 survey in Canada found that 4 percent of men and women reported being victims of spousal violence in the previous five years. However, less than 20 percent of male victims will tell the police or a health professional about the abuse. According to BLS statistics, only 2 percent of men who died of workplace violence in 2016 were killed by a domestic partner or relative. That is not to say, however, that men are less likely to be victims of intimate partner violence, Cawood says.

Organizations should provide a confidential conduit for employees to disclose concerns or abuse.

"Since 1985, the U.S. government and Canadian government have known that the initiation of physical violence in intimate partner relationships is identical by gender," says Cawood. "The number of cases where someone starts a physically violent event is equal by gender, but the harm is not equal. When a female is a target, the odds of her getting hurt physically are significantly higher, but the initiation rate's the same.... From a threat assessment perspective, I have to recognize that I can't look at gender and immediately know who the victim is and who the aggressor is. I have to be much more thoughtful about looking at the behavior and seeing what the context is."

REPORTING RISK

As with active assailants and other workplace violence incidents, early warning of potential risk is key to deploy-

ing an effective, proportionate response.

Like workplace violence in general, domestic abuse bears a variety of warning signs—both for the perpetrator and the victim. These can include aggression, personal crises, sudden shifts in mood, or injuries. Someone who is normally bubbly and outgoing becomes quiet, withdrawn, and isolated, or begins wearing concealing clothing such as dark sunglasses or long sleeves in the summer.

Think of warning signs as a theme, not a checklist, says Cawood. For example, when employees are required to report verbal or written threats, they may waver on reporting intimidation or other borderline warning signs, thinking they do not meet the threshold.

"When in doubt, just tell us. If you're uncomfortable, tell us. That way we break down those barriers," he adds.

On signs of abuse, the employer can make an effort to reach out in a compassionate, confidential, and non-presumptive way, Curtis says.

"It's appropriate to allow the employee to know that you're concerned for their well-being and that you're there to provide assistance if they need assistance," he says. "Oftentimes the employee will begin to open up, and you can see what you can do to help. Sometimes the employee may just deny it outright. In that instance, it's difficult to take very direct measures, but you should still be circling back to the checklist of security items in your workplace violence program to make sure, for example, that the building is secure, that all of the lighting in the parking lot is working, that this employee knows that if he wants an escort to or from his car or whatever the situation may be that those things are available to him. Encourage them to reach out to you. Even if in the first conversation, they're not comfortable disclosing anything, keep that chain of communication open."

To encourage communication and reporting, Curtis adds, organizations can offer more than one means of coming forward with information—employees have different comfort levels with different people, and offering them multiple channels of reporting makes them more likely to do so.

"Make it clear that you are genuinely concerned, and make it clear there will be no retaliation for coming forward," he says.

However, if there is a concern for real violence, safety trumps confidentiality, including in sensitive matters such as IPV. Even employee assistance programs and psychologists have a responsibility to protect potential victims if people disclose direct threats or pose a serious danger of violence to another, as decided in the United States through the 1976 Tarasoff v. Regents of the University of California ruling, says Michael A. Crane, CPP, an attorney and security consultant with Securisks. Crane is also a member of the working group revising the ASIS Workplace Violence Prevention and Intervention standard. If a manager or other organization official learns about a potential threat and does not respond with appropriate action to mitigate risk and protect potential victims, the organization could be liable if something occurs.

In addition, workplace safety regulations in the United States, Canada, and some European countries require organizations to respond to realistic expectations of violence—whether related to IPV or other forms of workplace violence—as they would to any other hazard, seeking to minimize employee injuries and other collateral harm, he says.

This also extends, in some countries, to remote workers. "In both Canada and the United States, there are now regulations and obligations that talk about the need to protect

individuals when their assigned workplace is their home," Cawood says. "So I'm sitting at my kitchen table working, and my spouse comes home and starts hurting me. There's an obligation now for the organization to both assess and decide if there are things we need to do to protect that individual during working hours."

The first line of workplace violence risk mitigation is reporting, but this will always be a challenge around domestic abuse.

However, the challenge to learn about threats remains: "People are still uncomfortable getting involved in other people's relationships," Cawood adds. "We can't tell people what to do in their personal relationships, and nor should we. But at the same time, how do we balance the obligation we have to help aid in their safety against the idea that they have freedom of choice about who they maintain contact with or how they decide to work out their personal life?"

TRAINING

The first line of workplace violence risk mitigation is reporting, but this will always be a challenge around domestic abuse. "The more personal or private people perceive a problem to be, the more difficult it is to manage within an organization," Cawood notes.

To circumvent cultural challenges around reporting workplace risks stemming from other employees' personal lives, organizations can incorporate IPV into overall workplace violence training. When giving examples of workplace violence, weave in details about how domestic partners could also cause workplace violence incidents, not just outsiders, customers, or employees.

"Normalize the idea that behavior is the issue, and no matter where it comes from or how the person is connected to the workplace, there's going to be this expectation that people will pay attention and report it," Cawood says.

The warning signs are similar, so training sessions—both for new hires and refresher courses—can echo many of the same themes. For aggressors, is the person experiencing a financial or health crisis or a substance abuse issue? Do they have a personality disorder, or act domineering or controlling? Do they make threats or intimidate others to get their way? "These are the warning signs for any type of person on a pathway from thought to action for violence, but what you want to do in your training is weave in the idea that this could happen from a domestic partner, a former or current boyfriend or girlfriend, or a casual encounter," he says.

THREAT ASSESSMENT

Threat assessment for IPV differs slightly from violence risk assessment, says Cawood; in a threat assessment, a multidisciplinary team consisting of security, HR, legal, and other stakeholders makes determinations about victim safety based on behavioral context, instead of making judicial or punitive decisions.

"It's about looking forward: what could happen, and how do we begin to prevent it?" he says. It's also a matter of advising without dictating.

For example, Cawood says that when advising an employee about restraining orders, the threat assessment team should explain the process, hearings, time delays, and enforcement to give the victim a realistic understanding of the system. Afterward, the employee is free to make his or her own determination of whether or not to proceed.

"Educate them in a very neutral way," he adds. "There

are significant numbers of cases in intimate partner violence where seeking a restraining order can be very helpful. But there are also a significant number of cases where—at that moment—seeking a restraining order does nothing but accelerate the risk."

Threat assessors should understand that IPV, especially when it includes a spouse or long-term partner, involves many other connections and complications: family, children, finances, shelter, and emotions.

"One very positive thing businesses can do other than educating individuals in situations like this is taking responsibility for doing assessments and appropriate interventions," Cawood says. For example, an employee at risk could be moved from an outward-facing customer service position that makes them accessible to individuals walking in off the street to a more secure role. If the intimate partner has been making threatening phone calls to the employee's work phone, consider rerouting telephone calls for that employee through a supervisor or security professional to screen calls and document ongoing threat pattens.

In addition, the organization can put the person in question on notice by issuing them a letter of expectation. These letters communicate that the employee's personal decisions outside of the workplace are their own, but as part of the organization, they have a responsibility to help keep coworkers safe. Therefore, Cawood adds, if a relationship change occurs, police are called to the employee's residence, or if the threat level changes, the employee has an obligation to inform the organization about those changes so the threat can be reassessed and managed.

HR or security professionals can proactively reach out to the potential aggressor, inform him or her about recent reports or concerns, and begin a dialog with that individ-

ual. This may even de-escalate the situation because the perpetrator is less interested in pursuing their partner when other people are involved.

If the offender is an employee, Crane advises potentially suspending that person with pay while an investigation is conducted. If the employee's actions or threats violate company policy or codes of conduct, that person can be disciplined up to and including termination.

"When you're talking about a potential threat, you want to create a termination that will not cause more problems," he says. "So you want to see what can be done—whether it's money or continued medical coverage—to create a soft landing. This person has existing problems and you want to get them out of the workforce, but you want to create an environment where they won't come back, because they're happy. HR and security can create a package that will hopefully eliminate risk."

It is helpful to establish standardized security and IPV response protocols in advance, Crane says. "What you do for one person, you then have to do for another person in the same category," he adds. "Companies can have a policy for every employee type, and actions can be taken based on the level of employment that person has." For example, Crane says that a threat against a CEO or chairman of the board might warrant executive protection, while the obligation to protect an administrative assistant outside the workplace may be lower. But consistency and transparency are essential.

Domestic abuse cases are evolving situations, Crane notes, and they can change mid-investigation or even post-investigation. It is not uncommon for threats to be sent in long after initial action has been taken or even after a person has left the company. Continuing to monitor individuals' social media presences for threatening behavior

and keeping an archive of communication helps to keep the organization informed.

Even if a perpetrator has been arrested, the threat assessment process continues. In most cases, the individual will be released from custody eventually, and active monitoring of cases is necessary so organizations are not surprised when a threat resurfaces, Cawood says.

Crane adds: "Among threats in the workplace, workplace violence threats are probably the number one category, and the majority of them are domestic-related. So it is an issue that spills into the workplace. And the reason to prepare and have programs in place is that the offender—whether it's an employee or an outsider—always knows where the victim is when they're at work."

CLAIRE MEYER IS MANAGING EDITOR AT SECURITY MANAGEMENT. CONNECT WITH HER ON LINKEDIN OR CONTACT HER AT CLAIRE.MEYER@ASISONLINE.ORG.

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.