HOLISTIC THREAT-ASSESSMENT STRATEGIES

MITIGATING AND MANAGING THREATS AND ACTS OF VIOLENCE

By Steven C. Millwee, CPP

Loss prevention and retail executives' careers are dramatically altered when violent crime impacts their business. The loss of human life, coupled with the loss of trust by coworkers and senior executives, puts careers in jeopardy when on-the-job murder or violence strikes. Whether the homicide or acts of violence are the result of an armed robbery, a loss prevention agent attempting to make a shoplifting stop, or a disgruntled employee going "postal," the financial and emotional fallout impacts the entire enterprise. Implementing a multidisciplinary or holistic approach to help mitigate the risk of violence allows every stakeholder to be part of your proactive policies, procedures, hiring practices, and threat-assessment strategies.

Though human resources, security, and loss prevention have learned to team together in many areas, collaboration over workplace violence threat assessments remains an area for improvement. Learning how to leverage the skills of internal and external experts is essential to a sound violence-mitigation approach, as many crimes are reasonably foreseeable. Where violence is foreseeable, plaintiff's experts will argue it was preventable. The past is the best predictor of future behavior.

A Proactive Strategy

Most organizations wait for legal counsel to retain expert witnesses only after lawsuits for negligent hiring, security, supervision, premises liability, false arrests, and failure to warn are upon them. Yet enterprising retailers do not wait for tragedy and subsequent litigation to strike, as they have experts already in place. Integrating experts into the retailer's culture, policies, procedures, and practices forms a proactive strategy that prevents workplace violence.

Following is an example of changing management behavior to proactively prevent violence incidents.

Mary, a 15-year, trusted associate, arrives at work with two black eyes. She is wearing clothing to cover her arms, though that is not her summer style. Her female manager finds her in the restroom…in tears.

Mary pleads, "I need to tell you something, but you must promise to keep it a secret. No one can know. It's very personal."

One skill set we expect of our managers is their empathy and approachability. Yet, agreeing to keep Mary's secret without knowing the context or content should never be promised. Often the request for secrecy finds its genesis in an employee's embarrassment. Yet, the employee is looking to a trusted manager as a cry for help.

A proper response is, "Mary, you know that I care about you. You know that I am a person of integrity and committed to always trying to do the right thing. Tell me what's happening, and I will commit to you that I will discuss with you what can be done and, if I can, keep the information private. If I can't, I'll explain why I cannot. I am confident that we can find the solution together." You will find the employee will still tell you what is impacting her life.

The Threat-Assessment Team

Forming a threat-assessment team long before acts of workplace violence occur has a return on investment; as threats and acts of violence are eliminated, risks are mitigated, and employee morale and trust in management helps reduce turnover and increase productivity. Every employee expects to be safe at work, and the law demands it.

Whether the homicide or acts of violence are the result of an armed robbery, a loss prevention agent attempting to make a shoplifting stop, or a disgruntled employee going "postal," the financial and emotional fallout impacts the entire enterprise. Implementing a multidisciplinary or holistic approach to help mitigate the risk of violence allows every stakeholder to be part of your proactive policies, procedures, hiring practices, and threat assessment strategies.

Retailers, large and small, should consider the following individuals and roles and responsibilities when forming or updating their threat-assessment teams.

Rule #1—Avoid the "brain-drain syndrome" by rotating employees without professional training off the threat-assessment team. Mentor each new member for a year or two through several events so that the rules

of the road, policies, procedures, and best practices are integrated in a cohesive manner. Every employee must receive workplace violence prevention training, as they are the eyes and ears of the organization. An employee who does not know what to look for, report, and to whom to report longstanding warning signs deprives the retailer of the most important early-warning device. In a negligence lawsuit, the employer cannot rely on a "we didn't know" defense strategy, as employees reveal the history of threats, violence, and other aberrant behavior to law enforcement, through depositions, and to today's 24/7 news cycles.

Rule #2—Use a multidisciplinary approach in forming the team. One prominent retailer stacks their team with senior executives from loss prevention, HR, legal, operations, and employee assistance (EAP), along with two outside experts.

Rule #3—The first expert is the workplace violence threat-assessment and intervention consultant. The organization must select an expert who knows how to perform threat assessments and evaluate the propensity for violence. They should have the ability to interview employees to maximize content and compose evidence-laded interviews, and be able to perform the formal threat assessment and intervention interview of the subject and employees.

Some retailers will interview the suspect, which typically results in denials, half truths (which are whole lies), and answers filled with faulty memories or attempts to blame the victim, all of which are counterproductive. Skilled threat-assessment experts with experience in hostage negotiation and violent-crime interviews are able to develop a rapport that results in admissions and confessions. Often this expert interviews employees and the victim of the threats or violence, as their experience and skills will identify additional facts that employees may be reluctant to admit to a manager. Though many LP and HR professionals have the skills and experience, using an outside expert transfers the subject's violent ideation away from the retailer and management.

Rule #4—The second expert is the operational psychologist. This person applies psychological theories and models by viewing the threats or acts through the eyes of the operator, often threat-assessment and intervention experts and trained investigators. According to clinical psychologist Russell Palarea, Ph.D., "The focus of operational psychology is to provide psychological knowledge, skills, and abilities to the operational mission." An indirect psychological assessment leverages the intervention and interviewing resources to better understand the motivations and pathologies. Assessments should be focused on collecting more

facts that lend to defusing the threat. It is ill-advised to use clinicians or academia-based psychologists versus operational psychologists.

Clinical tools fail because the mental illness may be unknown or nonexistent, and clinical techniques, such as interviews and psychological tests, may provide partial, inaccurate, or irrelevant information related to the potential act of violence. Absent written consent from the subject or court order, clinicians have HIPPA medical privacy restriction and are limited by various laws based on the imminent threat the individual poses to others and himself.

Organizations must also be careful how they implement employee assistance programs (EAP), as the unintended consequence could result in Americans with Disability Act and privacy claims. Operational psychologists are adjunct experts that can provide important insight into life stressors, non-verbal cues, tone, inflection, and mood communication. Content and context of words used helps the intervention team assess the subject's logic and decision skills, if any.

Although human resources, security, and loss prevention have learned to team together in many areas, collaboration over workplace violence threat assessments remains an area for improvement. Learning how to leverage the skills of internal and external experts is essential to a sound violence-mitigation approach, as many crimes are reasonably foreseeable.

Rule #5—The threat-assessment team must be empowered to act. Assessments are time-sensitive. Risk mitigation and intervention plans cannot wait for a senior executive briefing and delayed decision cycle. Some teams use a consensus style, while others appoint a senior member or another member of the team to become the final authority, usually based on availability of team members and areas of expertise. However, the team should never ignore threats or an act of violence, as allowing the offender to remain on the job exposes employees and the public to violence, particularly if the offender fails to comply with the teams' mandates. The team takes on tremendous responsibility, and as such, can never use plausible deniability and testify they were outside the loop.

Rule #6—Preserve all evidence, records, and reports. The retail environment generally has multiple security video recordings that must be immediately preserved. One recent workplace violence case that resulted in litigation revealed through depositions and documents that several security and non-security managers viewed the video of the attack, but failed to download the recordings. The defendant claimed that they attempted to download too large a file, had not updated their software since installing their CCTV system, and then allowed the system to record over the date in question.

Imagine a jury's suspicion over the integrity of the company's witnesses in this scenario, as preserving evidence is a founding principle of any investigation. Juries often view the lack of documentation as definitive proof that the employer destroyed or hid critical evidence.

Documentation and preservation is your salvation. Moreover, always archive every workplace violence investigation, threat assessment, report, and all evidence. Whether you will need such in defending your enterprise in litigation cannot be known, but you have a greater probability of needing the files if the person acts out violently and law enforcement arrives needing your institutional memory to help defuse a hostage crisis or solve a violent crime.

Rule #7—Voluntary separation over involuntary termination is an essential long-term risk mitigation strategy. The natural reaction in the face of threats or acts of violence is to immediately fire the offending employee before an investigation and threat assessment is performed. Firing the worker ensures there is a loss of contact and loss of opportunity for rapport with the offender.

On the contrary, skilled threat-assessment intervention negotiators know how to obtain admissions and lead the offender to a voluntary resignation. This allows the employee to leave with dignity, appreciation for work contributions, and creates a mind-set of unmerited mercy. *Unmerited mercy* is giving compassion that the offender does not expect and rarely deserves because of their disruption to the workplace. Yet, leaving voluntarily with

a sense of being treated with fairness and respect leads to a restoration of self-worth and allows the employee to reflect on personal accountability.

Rule #8—Pre-employment and periodic employee background checks are industry standards. Some retailers elect to perform background checks for select positions, such as management, finance, and loss prevention. However, workplace-violence offenders cannot be categorized by job title. When workplace violence strikes, after-the-fact police investigation often finds the proverbial smoking gun through an employee background investigation.

As of January 1, 2013, employers who use consumer agencies or background screening providers to conduct background checks on their applicants and employees must use updated versions of the FCRA's Summary of Consumer Rights form. The updated version complies with changes implemented by the newly created Consumer Financial Protection Bureau (CFPB). The updated model form is available at Appendix K of 12 C.F.R. § 1022 and can be accessed on the CFPB's website, consumerfinance.gov.

When you use background or consumer reports to make employment decisions, such as hiring, promotion, or termination, they must comply with the FCRA. The term "consumer report" is defined broadly by the FCRA and includes criminal background reports, credit history reports and other background checks. Under the FCRA, the Summary of Consumer Rights form must be provided to an applicant or employee when, among other things, a pre-adverse action notice is sent.

Treating the subject of the background check with dignity and transparency is essential to avoid the growing class-action background screening lawsuit trend. Always obtain written consent from the applicant or employee before performing a background check. A growing number of government agencies and employers are adopting a new de facto compliance standard, as it closely mirrors the new FCRA and EEOC mandates.

Ensure that your Consumer Authorization executed by applicants and employees allows you to periodically perform background checks without further notice or consent before the check. An essential step in a threat assessment is updating the background check. In this investigation, you want to look for potential landslide motivations for the behavior. Recent divorce petitions, restraining orders, violation of such orders, bankruptcies, and police reports are additional resources for a threat-assessment background check.

Counsel can guide you on jurisdictions that may restrict post-employment background checks. In some cases, counsel may instruct you or your provider to perform the check and have the report returned to their

law firm. Counsel may restrict this report to the outside threat-assessment professionals, where the content and context is necessary for their evaluations. Counsel may label the threat-assessment background report as "attorney-client work product" and instruct you to not send the results to the employee or subject.

However, the skilled threat-assessment professional can often use the report during the interview or intervention phase. The report, FCRA rights, and adverse action letters, if any, can be given during these phases. In instances in which the subject has paranoid thoughts or delusions about your company, employing this approach will mitigate risk when you are required to send them their background report in compliance with the FCRA.

In more serious instances, law enforcement may perform the background check as part of their investigation. Law enforcement background checks are not covered under the FCRA unless you ask that the report be prepared or given to you, which may have the unintended consequence of it becoming a consumer report as defined by the FCRA.

Loss prevention and their HR team should work together to update background investigation policies and procedures. ASIS International and Society for Human Resource Management (SHRM), along with the input from multidisciplinary experts, have published several important standards, including workplace violence prevention and background screening best practices. Careful review of these standards will help you mitigate risks and ensure compliance with best practices.

Rule #9: Future-focused prevention is essential. Few employers reinvestigate the criminal histories of existing employees, except during misconduct, threat, workplace violence, or harassment investigations. Portions of the U.S. military have adopted a unique program for future-focused crime prevention. Employees and vendors seeking ongoing access to military bases must pass a background investigation not just once, but every year and every three months.

"[The military] realizes that a person may be convicted of a crime after initially being approved for access, which can only be detected through ongoing re-investigations," says Jim Robell, innovator of the program. This forward-thinking company and companies like it pave the way for the future of risk management and security.

"Knowing who we hire and allow access to, while ensuring transparency and accuracy, is the new standard in hiring and risk avoidance," says Raymond Humphrey, CPP, past president of ASIS International. "The latest tool to ensure compliance with the FCRA and EEOC mandates helps mitigate the growing number of federal and class-action lawsuits."

Rule #10—Avoid the failure to warn and no-trespass agreement landmines. Many employers conduct a threat assessment that leads to the voluntary separation or firing of an employee over acts or threats of violence, but fail to communicate to employees that the offender is no longer welcome in stores or on corporate property. Many ask, "Are we setting ourselves up for defamation, slander, or liable claims as only select employees, such as managers, may have a need to know?" Others ask, "What about employee privacy?"

A well-crafted severance agreement incorporates a consent by the employee or subject giving you or your experts written permission to communicate with their former coworkers. Remember, if the matter involved instilled fear or criminal acts or threats of violence and stalking, you have potential long-term exposure to future violent retaliation. Following is language often used by this author in voluntary separation and severance agreements:

To ensure the safety and security of the company and our employees, you agree to not return to any corporate offices of our company without the written consent of

continued on page 22

Employees look to their leadership to provide a safe and secure workplace. Hotlines, website reporting, avoiding whistleblower retaliation, and using longstanding threat-assessment strategies are essential to a loss prevention program. Making every employee part of the solution empowers everyone to be part of the workplace violence prevention team.

continued from page 20

Steven C. Millwee, our consultant. You further agree to not telephone, email, text, or communicate with any of our employees in a manner that would be considered harassment, unwelcome contact, threatening, or in violation of any law.

You agree that where any employee of our company communicates his or her desire to have no contact of any kind with you, that you will cease all attempts to have contact or communication with said employee. You further agree that the company or its agents, such as our consultant, may communicate with any employee or other party about you as it relates to your agreement to not trespass on company properties, including all retail stores of the company or its franchises. You agree that a violation of your agreement to not trespass on company or employee properties (where they have communicated instructions to have no contact with them) may lead to you being subject to arrest for Trespass after Warning in violation of applicable state, federal, or municipal laws. You agree that this entire agreement may be used by law enforcement as evidence that you received proper legal notices regarding violation of the no contact or trespass provisions.

The threat-assessment professional is trained in explaining the severance agreement and specifically the reasons for a no-contact or trespass warning. A common example may be as follows:

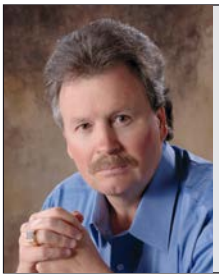
"Joe, I appreciate you having taken responsibility for your statements and, as you have asked me to tell your coworkers that you would never harm them and want me to apologize to them for causing them to be afraid of you, there is a special way that I can do this. The steps I'm about to explain help hold you accountable to your agreement to never bother, harass, or harm our employees or others related to the company, but it allows you to see how I communicate this with the same sense of compassion and unmerited mercy concept we have been talking about.

"Joe, what I generally say to the employees in meetings or written communications is something like this—'Joe voluntarily resigned his employment and wanted us to communicate this very personal message in his behalf. He asked that you forgive him for his misspoken words or inappropriate acts, as he has had time to reflect on many factors that brought him to a moment of clarity. He takes personal responsibility and chose to resign his employment to make you feel safe. He wanted us to communicate that he is not angry and has no intention of harming you or anyone. He wants to leave with dignity, and as such, has asked that you not contact him or ask him about his reasons for leaving. Doing so would only make him feel bad and violate his desire for privacy and respect. Joe has no intention of calling, texting, communicating, or emailing you in any form unless you personally wish to continue your friendship in writing. However, the company restricts Joe from talking to you about this matter and he intends to abide by his agreement. Joe did the right thing and should be commended and remembered for the many good things he did while with the company. He stood tall and took personal responsibility, has apologized, and is moving forward in a positive direction. Please only say good things to others about Joe, as speaking badly only creates opportunities for future avoidable problems. Lastly, you should be very proud of your company for their willingness to communicate Joe's message, as most employers never talk this openly about such a sensitive subject. Your company treated Joe with respect and dignity. He has written a personal apology to the company, as he wants everyone to be safe, secure, and able to move forward in a positive way. He commented during this difficult time how he appreciated the company and his managers and coworkers, as he was not cast out but allowed to leave with respect and dignity.'"

Proactive versus Reactive

These proactive steps, along with using a formal threat-assessment tool, such as SecurThreat, are resources every retailer should consider. The purpose of threat-assessment teams is workplace-violence prevention. The absence of a team, planning, and on-going training leaves your enterprise vulnerable.

Employees look to their leadership to provide a safe and secure workplace. Hotlines, website reporting, avoiding whistleblower retaliation, and using longstanding threat-assessment strategies are essential to a loss prevention program. Making every employee part of the solution empowers everyone to be part of the workplace violence prevention team. ■



STEVEN C. MILLWEE, CPP, is a highly-regarded expert witness with more than 34 years of experience testifying in high-profile cases. He has performed thousands of threat assessments and has been an intervention expert responsible for negotiating with threatening or violent offenders for both small and large retailers, Fortune 500 corporations, and various federal and state government agencies. A frequent trainer, Millwee invented and patented iReviewNow, which is designed to protect employers from EEOC and FCRA litigation. Formerly with the FBI and a past unsolved-murder detective, he is the current president and CEO of SecurTest, Inc., a leading background screening provider. In 2002 Millwee served as president of ASIS International and was on the founding editorial board of *LP Magazine*. He is the coauthor with labor attorney John-Edward Alley of *The Threat from Within: Workplace Violence* (1995). He can be reached at smillwee@securtest.com or 800-445-8001.