Journal of Threat Assessment and Management

Imagining the Unimaginable to Prepare for the Unthinkable: Criteria for Detecting, Reporting, and Acting to Thwart Intended Violence

Frederick S. Calhoun and Stephen W. Weston

Online First Publication, February 27, 2023. https://dx.doi.org/10.1037/tam0000200

AMERICAN PSYCHOLOGICAL ASSOCIATION

Journal of Threat Assessment and Management

ISSN: 2169-4842

https://doi.org/10.1037/tam0000200

Imagining the Unimaginable to Prepare for the Unthinkable: Criteria for *Detecting*, *Reporting*, and *Acting* to Thwart Intended Violence

Frederick S. Calhoun[1] and Stephen W. Weston[2]

[1] Arlington, Virginia, United States

[2] Pioneer, California, United States

"Imagining the Unimaginable" addresses the need for organizations to establish a process for detecting inappropriate behaviors and reporting them to entities capable of acting on the reports. The article recommends incorporating threat management concepts into law enforcement training curricula. It advocates establishing reporting procedures and identifying trained "designated receivers" within the various venues to receive and act on the reports. It also offers an all-purpose reporting guideline keyed on the path to intended violence that proposes "All Threat—All Reporting" criteria, serving as an educational tool for training everyone within law enforcement and different venues. Finally, the article explores the different responses needed for critical and noncritical threats. Together, these recommendations address the challenges involved in initially identifying problem individuals so that the threat management process can begin.

Public Significance Statement

This article is significant because the detecting, reporting, and acting process it recommends fills the current void between the occurrence of a threatening or ominous act and the initiation of the threat management process of identifying, assessing, and managing problem individuals. The article also offers model criteria for what types of behaviors should be reported and recommends ways to train individuals on those criteria.

Keywords: detecting, reporting, acting, reporting criteria, threats

Over the past several years, the authors have grappled with one of the most overlooked problems in the field of threat management—how to identify individuals who are potentially intent on violence. Our chapter contribution to the second edition of the *International Handbook of Threat Assessment* briefly sketched out our developing ideas, which we framed as the *Detect, Report, Act* (DRA) *Process* (Calhoun & Weston, 2021). A year later, we explained that concept to chiefs of police and other law enforcement managers (Weston & Calhoun, 2022). In the present article, we explore the model in more detail, with a particular emphasis on the proper role of law enforcement and how that role changes depending on the imminence of the risk. As the violence looms ever nearer, the need for law enforcement involvement increases apace. The DRA model tries to intercept subjects intent on violence long before they reach the violent stage. To do so, the model depends on early identification of problem subjects.

Frederick S. Calhoun https://orcid.org/0000-0003-0605-0212

Stephen W. Weston https://orcid.org/0000-0002-2925-5360

This article addresses the challenge of detecting potentially violent individuals before they commit a violent act. It proposes a process for *detecting, reporting,* and *acting* on indications of violence-prone behaviors. As part of that process, the article offers a generic, one-page broadside for use in educating individuals on the types of problematic behaviors to report.

Correspondence concerning this article should be addressed to Frederick S. Calhoun, 2146 Military Road, Arlington, VA 22207, United States. Email: fcalhoun@comcast.net

As an integral part of identifying individuals intent on violence, we developed a generic, single-page broadside focusing on behaviors indicative of future or potential violent acts. We offer these "All Threat—All Reporting" guidelines as a model for organizations to use to customize their own warning signs specific to their environment. The criteria are organized along the path to intended violence, a simple and easily understood analogy for thinking about the progression violent individuals follow to launch their attacks. Those attributes make the criteria ideal for educating everyone within a venue on what behaviors need to be reported.

At the outset, we recognize a complicating factor involved in attempting early identification. Based on our respective experiences and observations as threat management practitioners for over 30 years each, law enforcement usually requires an actual crime to occur before they act. The police are primarily empowered to address criminal acts and maintain public safety. Yet, in reality, law enforcement is the ultimate default receiver of threat issues and, in critical situations, becomes the ultimate crisis manager. Frustratingly, threat managers may identify potentially violent subjects, yet find themselves barred from employing a law enforcement management strategy because their early identification did not derive from that subject committing a crime. In our opinion, the solution depends on training law enforcement officers at all levels in the rudiments of threat management, thus opening the door to violence intervention rather than judicial punishment. We recommend that the threat management community at large should embrace that entry.

Yet, another challenge to identifying subjects of concern early on, in our experience, derives from the natural inclination in setting up security protocols to assume who or what should be the likeliest potential target. In corporations, the perceived likeliest targets tend to be chief executives and other high-profile persons. In governments at all levels, high-ranking elected officials seem the most vulnerable. This tendency erects blinders to the potential for other types of violence to occur in any setting. Corporations and governments, for example, should also be alert to the potential for domestic or workplace violence. Either may become targeted as a symbolic or representative quarry. Consequently, the "All Threat—All Reporting" criteria maintain a broad reach to capture as many indicators of potential violence as possible.

The prevailing doctrine in threat management describes the process as consisting of three steps: *identifying* problem individuals or situations, *assessing* their degree of risk, then *managing* the individuals or the situations to defuse the potential risk (Amman et al., ca. 2016; Calhoun & Weston, 2016; Center for Prevention Programs and Partnerships, 2021). Issues related to proper assessment techniques, including computer-assisted programs, have long captivated the field's attention (see Cawood et al., 2020; Cooke & Michie, 2014; Gerbrandij et al., 2018; Hanson et al., 2014; James et al., 2022; Jung & Himmen, 2022; Meloy & Gill, 2016; Storey & Hart, 2014, for a sampling of such interest). Identifying has not received nearly as much attention. We believe it is time to pay more heed to the difficult task of initially identifying subjects of concern by their problematic behaviors signifying the potential for future violence.

Identifying precedes the other stages of the threat management process. Without first recognizing the problem individual or situation, assessments—computer-assisted or not—have nothing to assess. With no assessment, no management plan can be put into play. Failing a timely identification stalls the threat management process until the threat situation becomes so critically dire as to put lives at risk and require urgent law enforcement intervention (Calhoun & Weston, 2016, 2021; Weston & Calhoun, 2022).

The entire threat management process hinges on the initial identification of the potential problem. Neither the threat manager nor any support team can act until they recognize the behavior as a potential threat. Identifying problem individuals or situations early gives more time to conduct thorough assessments while retaining a wider range of management options available to threat managers for defusing the risk. The DRA model (Calhoun & Weston, 2021; Weston & Calhoun, 2022) provides a way for early identification. The threat management community as a whole, and law enforcement in particular, needs to prepare itself to utilize the opportunity early identification offers.

The relative dearth of threat management professionals nationwide further exacerbates the delay in implementing the threat management process. In our respective experiences, few organizations have access to threat managers, much less designated threat management teams of subject matter experts on call for any emergency. That luxury, it seems to us, extends far beyond most organizations' capabilities or interests. Instead, individuals

with little or no training or experience in threat management are confronted with reports of threatening behavior or suspicious activities that are not criminal. Among businesses and corporations, these "designated receivers" of potential threat information tend to occupy positions in legal or human resources departments. They are more accustomed to opining about the law or doling out discipline, hiring and terminating personnel, and plotting career paths than managing threats. In schools, the designated receivers are usually guidance counselors or school resource officers. The former focus most of their time on career counseling and educational planning advice; the latter on general policing and security of the premises and their occupants. Schools tend to place more emphasis on interaction and early intervention with problem students. Unfortunately, some communities want little or no law enforcement presence in their schools and have evinced significant pushback against assigning school resource officers. Although, as the roster of the Association of Threat Assessment Professionals (ATAP) readily attests, many of these designated-receiver types are actively seeking training and professional certification as threat managers, their numbers across the nation remain seriously low.

Based on our experiences and observations over the years, most entities do not even have designated receivers. Instead, they rely on what we call "default receivers." They receive reports of inappropriate behaviors because no one else is available to take them. The problem essentially ends up in their laps because the organization has not addressed the issue and no designated receivers have been identified. Default receivers are even more unprepared to handle threatening situations than designated receivers. This lack of trained or experienced threat managers within most organizations puts an even greater onus on law enforcement first responders to recognize and react at the moment when dealing with rapidly escalating situations prior to a criminal act occurring. In this article, we address the challenges emanating from the lack of qualified threat managers. ATAP, the preeminent organization in the field of threat assessment and management, has, as of June 2022, qualified only 198 individuals as Certified Threat Managers (Okada, 2022). Although more since then have met the stringent requirements for certification, the numbers remain staggeringly low given the nationwide increases in violence and violent attacks (Fisher & Keller, 2017; Mosbergen, 2022; "A Partial List of Mass Shootings," New York Times, 2022).

Some federal agencies, notably the U.S. Secret Service and the Federal Bureau of Investigation, have personnel experienced in evaluating threats. Private security consultants manage threat issues for those that can afford to consult with them. Many mental health practitioners have expertise in violence risk assessment. Yet, nationwide, the number of such trained or experienced threat managers remains paltry, certainly nowhere near the level necessary to adequately address, much less diminish, the problem.

In our experiences, most private organizations that cannot afford trained threat managers rely on untrained or superficially trained staff members—whether designated or default—whose daily experiences are completely divorced from violence and those who perpetrate it. They are unaccustomed to imagining the unimaginable. This fundamental reality convinces us to advocate minimum training programs designed to educate large numbers of people in law enforcement and among the private sector on the fundamentals of recognizing and reacting to threatening behaviors or circumstances. These threat management concepts and techniques facilitate preparing for the unthinkable.

The lack of trained or experienced threat managers does not make the situation hopeless. By comparison, heart disease, the leading cause of death in the United States, felled 696,962 Americans in 2020 (Centers for Disease Control, 2020). Yet, the specialists needed to combat this scourge—cardiologists—numbered only 18,610 as of May 2021 (Bureau of Labor Statistics, 2021). Instead, throughout the United States, private and public organizations provide training in cardiopulmonary resuscitation. Many buildings now contain automatic external defibrillators for quick use for anyone suffering a heart attack. Law enforcement and other first responders have a higher level of emergency medical training than they currently have in threat management. We urge that this be remedied by having all law enforcement personnel receive a minimal level of training in threat assessment and management techniques.

As with heart attacks, the danger caused by persons who pose a threat can also be addressed through training and widespread awareness of how to recognize relevant behaviors. As with programs helping to prevent heart attacks, awareness of the warning signs and symptoms is key (Meloy, 2015). We also address here those structures and

activities that must be in place *before* the traditional threat management process—*identifying*, *assessing*, and *managing*—begins. In more colloquial terms, we look at what must happen to increase the likelihood that a threatening situation raises alarms and allows the alarms to be heard by the right people. In urgent situations, law enforcement responds to any warning bells.

In addition to examining the process for getting to the identification phase, we further ask what needs to happen during those rare but increasingly deadly instances when the violence is not only potential but imminent. How should organizations and the individuals composing them screen for those situations requiring an immediate tactical response? Our respective experiences convince us that, in critical situations, the process of identifying, assessing, and managing usually happens "on the fly." The process unfolds as rapidly as the situation itself. That is, both the default and the designated receivers ideally recognize immediately the critical nature of the situation and the apparent imminence of the threat. They respond without either having or taking the time to convene a threat management team or conduct clearly articulated threat assessments. They respond to the emergency confronting them by adopting the best management strategy available at that instant. Even default receivers, those with no training and little experience, easily recognize emergency situations requiring immediate responses. Nonetheless, that type of situation and reaction needs to be factored into the threat management process.

Case Example

In the early morning hours of June 8, 2022, Nicholas Roske got out of a taxi near the home of Supreme Court Justice Brett Kavanaugh. Spotting two deputy U.S. Marshals standing post outside the house, Roske walked away from the residence. Minutes later, he called the Montgomery County Emergency Communications Center. He confessed to the operator that he was having suicidal thoughts and intended to kill a Supreme Court justice. He also admitted to having a firearm with him. While the operator kept Roske on the phone, the Communications Center dispatched patrol cars to Kavanaugh's neighborhood. Police arrested Roske before he ended the call with the emergency operator (Wolfe, 2022).

The contrast between the quick action taken in response to Roske's 911 call and the rather deliberative process of *identifying*, *assessing*, and *managing* that experts in threat management have advocated for so long caught our attention. Although most experts in threat assessment readily distinguish between imminent danger and potential risk, the difference between them raised an interesting point. What needs to happen before the threat management process even starts? That is, how do those who have to deal with threat situations get the information they need to even begin the identification process, much less conduct the assessments and select the appropriate management strategies? Clearly, the emergency operator who fielded Roske's phone call recognized the urgent nature of the situation and the imminent risk of violence to the justice. But no one stopped to convene the threat management team (if one even was available to respond), conduct a deliberative, well-thought-out assessment, and debate which management strategy best applied. Instead, the staff at the Communications Center recognized the imminent threat and issued the alert. Police responded and, within moments of Roske making his intentions known, arrested him, thereby neutralizing that particular threat.

Obviously, not every potentially violent subject calls 911, gives their location, and commits a criminal act by clearly announcing their intent to kill. Indeed, very few do. Often, many behaviors of concern, while still noncriminal in nature, are observed by others who do not understand their significance, or know how, or where, or even whether to report the suspicious activities. On occasion, even trained law enforcement call-center operators miss important indications of potential targeted violence. In 2017 and early 2018, Federal Bureau of Investigation "customer service representatives" working at the Public Access Line and supervised by special agents, missed two tips pointing to Nikolas Cruz as a self-described "professional school shooter." Both pieces of information, had they been managed correctly, offered the Bureau a chance to potentially intervene before Cruz killed 17 individuals at Marjorie Stoneman Douglas High School in Parkland, Florida, on Valentine's Day 2018 (McMahon & Wallman, 2018). That the customer service representatives and their law enforcement supervisors mishandled the two reports underscores how even trained designated receivers can drop the ball.

We can enumerate more examples of missed opportunities that ended in tragic results, interspersed with the occasional successful intervention, but doing so seems unnecessarily heartbreaking (Barnes, 2022; Jenkins, 2022; Therolf, 2019). Our respective experiences running threat management units repeatedly underscored the usefulness of one practical approach to threat management. Focusing on a subject's behaviors through the prism of the path to intended violence enables most individuals, once trained on this simple concept, to alert on suspicious activities, understand their importance, and sound the alarm. Doing so focuses attention on those behaviors in which all subjects intent on violence must engage in order to consummate an act of intended violence. Using the concept of the path and its integrated milestones—grievance, ideation, research and planning, preparation, breach, and attack—helps place suspicious behaviors within an easily understandable context that facilitates training, reporting, and initial response (Calhoun & Weston, 2016, 2021; Weston & Calhoun, 2022).

Our focus zeroes in on a practical methodology. That method extends across all venues of potential threat environments and targets, including workplaces or schools, gathering places, public figures, interpersonal relations, or symbolic or representational targets. These settings are not isolated from each other nor separated by hard and fast boundaries. Overlaps often occur. Domestic violence often occurs at workplaces; public figures become easier targets when they mingle amid public gatherings. Government facilities, including courthouses, carry the unenviable burden of being a workplace, gathering place, host to public figures, and symbol of government power, all rolled into one. From a threat management perspective, the challenge in each venue consists of devising an effective process for quickly identifying potential risks and the individuals who pose them.

The Detecting, Reporting, and Acting Process

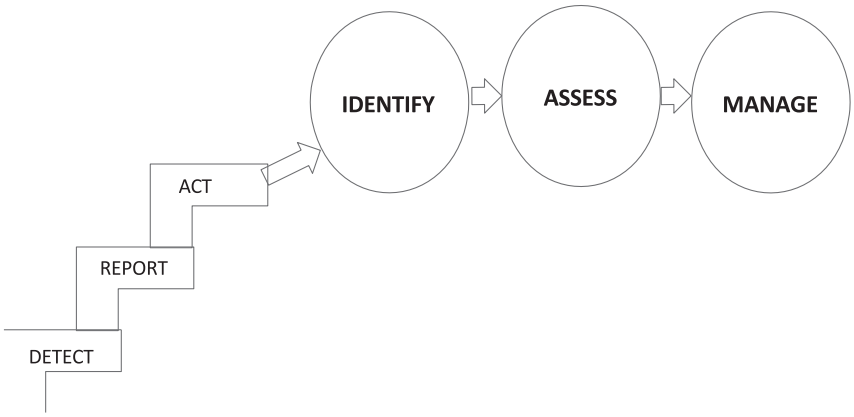
Regardless of the venues and each one's unique characteristics, the process for identifying risk remains the same. Establishing an effective procedure for identifying subjects who pose a risk of violence contains three vital components: detecting, reporting, and acting. These are the steps that must occur to get to the threat management identification stage, long before anyone can begin assessing and managing. Detection depends on identifying designated receivers well trained in threat management practices who will educate everyone within the venue on what, how, and where to report specific behaviors and situations indicative of potential violence. Processes for detecting are the fundamental groundwork that must be laid to ensure and facilitate timely and accurate reporting. Without this foundation, observable, path-related behaviors may never get reported. Reporting entails establishing methods and platforms for moving information about detected behaviors to the appropriate individual or organization. Acting means implementing the threat management process by identifying the potential threat, then initiating the assessment and management stages. It includes developing capabilities for responding to imminent potential violence.

Detecting differs from identifying. Detection occurs when someone within the venue recognizes behaviors described in the criteria and reports those behaviors to the designated receiver. After determining that the risk of violence is not imminent, the designated receiver then acts by identifying the nature of the threat and initiating the assessment and management phases of the threat management process. Detecting, then, is done by individuals familiar with the venue's reporting criteria but not trained or experienced in threat management. Identifying occurs when the trained designated receiver determines that some degree of risk exists and then invokes the threat management process.

Figure 1 illustrates how the DRA process melds into the overall threat management process.

Organizations, including law enforcement agencies, should design and establish ways to increase the opportunities to recognize relevant behaviors—those indicative of progress along the path to intended violence—and to ensure that those behaviors are reported to the appropriate entity that will act on the information, including with emergency responses when necessary. Any threat management system that lacks the fundamental DRAs risks never receiving or mishandling important indicators for discerning a subject's potential violent intent. If the subject cannot be first identified, then they can neither be assessed nor managed. The DRAs open the way for the threat management process to begin or, in time critical situations, the initiation of a timely tactical or investigative response.

Figure 1
DRA Process Leads to Identifying



Note. DRA = Detect, Report, and Act.

Detecting

Detecting a subject's path-related behaviors requires a coordinated effort across all aspects of the organization. That effort involves:

- assigning responsibility for designing and managing the threat reporting process, including establishing a point of contact for receiving information;
- crafting and disseminating specific criteria defining what behavior and situations need reporting and how and to whom that information is to be communicated; and
- training individuals affiliated with the organization on those criteria and communication methods with particular focus on personnel who interact with the public or the organization's external constituents.

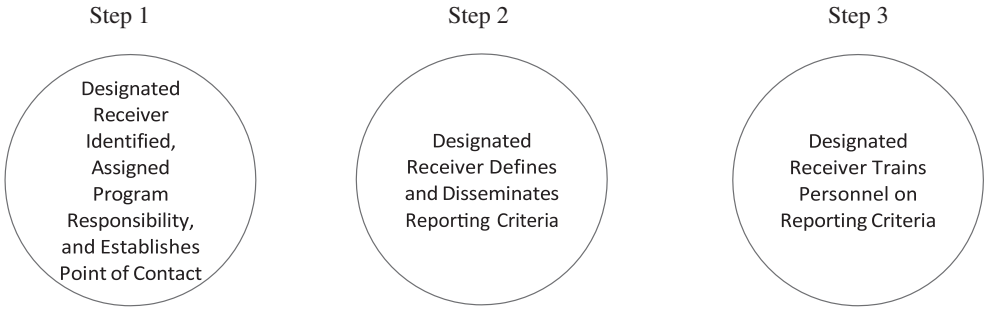
Figure 2 diagrams the steps required to set up a process for detecting those behaviors that need reporting to the designated receivers.

Implementing and maintaining these three steps ensure that the need to detect, report, and act on potential threat situations is addressed. The criteria delineate what needs reporting, assigning responsibility provides the place for the reports to go so they can be acted upon, and training on the criteria heightens awareness of potential problems.

Adopting Specific Reporting Criteria

Organizations, whether they be corporations, medical facilities, schools, government entities, places of worship, or social symbols, share similar, detectable risks. In the past, defusing those risks focused on protecting those perceived to be

Figure 2
Establishing Process for Detecting



the most likely target based on the type of venue. In government settings, governors, mayors, or other elected officials appeared the most probable target. In corporate venues, CEOs and other high-ranking executives received the most attention. Workplaces looked to employees as potential risks while schools zeroed in on students. Unfortunately, the focus on the perceived *likeliest* target and offender blinded organizations to other potential risks.

We recommend a more comprehensive All-Threat—All Target approach that avoids predetermining the source of the threat or the likeliest targets. In our respective experiences and observations, corporate security practices tend to focus on the company's executive leadership, critical infrastructure, and proprietary knowledge at the expense of attacks for ideological reasons or derived from workplace or domestic violence. We recommend, instead of assuming that the risk at large corporations focuses on the Chairman of the Board or Chief Executive Officer, a broader approach recognizing that the threat may be toward the company as a gathering place or representative target. It may come, too, from workplace violence among employees or domestic violence migrating into the workplace. For the public in general, security now requires imagining the unimaginable to prepare for the unthinkable.

In short, the criteria specifying what should be reported needs to cast a broad net precisely because those individuals who intend violence act from myriad motives that are highly personal and often obscure. Michael Louis, for example, returned to St. Francis Hospital in Tulsa, Oklahoma, to wreak revenge on the surgeon who failed to relieve Louis's back pain, as well as "anyone who got in his way." Louis succeeded in killing the doctor and three others before turning his firearm on himself (Abdel-Baqui, 2022). Focusing first on behaviors rather than presumed motives and targets allows the threat manager a wider perspective.

The broadside illustrated in Table 1 lists universal criteria for what should be reported. The criteria are organized according to the steps along the path to intended violence, that is, grievance, ideation, research and planning, preparation, and breach (Calhoun & Weston, 2016). The criteria are purposefully writ large to encompass as many behaviors of concern and communication methods as possible.

Having proper criteria is essential for several reasons. In our experience, most people will report information when they feel personally fearful or threatened, a very subjective test. They are less likely to report observable behaviors that they do not understand or recognize as indicative of potential violence. Problem behaviors that do not affect them personally may trigger a feeling of not wanting to get involved or cause trouble, a phenomenon long recognized as the "bystander effect" (Darley & Latané, 1968, Jenkins & Nickerson, 2017; Levine, 2012). They may ignore such behaviors as not their problem. They may minimize the behaviors, such as when coworkers react to angry outbursts by shrugging them off because "it's just Joe having another tantrum." Subjective biases based on stereotypes about particular groups or types of individuals may also result in no reporting at all or in exaggerated, unsubstantiated reports based on those prejudices. For example, inappropriate behavior by a well-regarded, high-performing employee or student may not be reported, while the same behavior in a low-performing individual might be reported simply based on the way each is perceived. The well-dressed individual may receive the benefit of the doubt, while the grungy guy might not. Well-defined criteria obviate these superficial biases.

Specific criteria both educate and overcome personally subjective decisions on what to report. For example, without well-defined criteria, a teacher may ignore a student exhibiting reportable behavior because "they are just looking for attention." Training that teacher on what they are required to report helps overcome that complacency. The criteria focus on concrete behaviors that are observable by those positioned within or around the organization. The criteria provide consistency across the organization and offer a complete encapsulation of what should be reported. The criteria provide a reasonable, defensible threshold for what behaviors will prompt a report and any subsequent action. Finally, they should be incorporated into a policy statement of the organization's mandate as to how it will respond to troubling behaviors. What is most important is that any criteria established be distributed, advertised, posted, and reinforced with training. It is of no value if nobody knows it.

Training

Designing an effective training program depends on the type of venue in which the training will take place. Some venues—such as workplaces

Table 1
Reporting Criteria

All threat—all reporting criteria

The following criteria apply to observed behaviors or reported contacts from an individual or individuals acting in concert received by any method of delivery, including, but not limited to, verbal, written, telephone, fax, text, email, all types of social media, Instagram, instant messaging, information from a credible informant, or obtained from diaries, videos, or audio recordings.
The criteria apply when the behaviors or contacts concern any target, including an individual; groups of individuals identified by the group's association, sex, race, religion, sexual orientation, national origin, family connection, social standing, or specific location; type of locale, geographic region, or the general public at large.
Report all threats of physical harm made by any method, whether direct, veiled, or conditional, concerning any target. Threats may also be nonverbal or implied by behavior or pattern of conduct.
Indicators of grievance
- *Any extraordinarily problematic* terminations, suspensions, expulsions, disciplinary measures, or denial of service, preferably prior to final implementation by the organization against the subject.
- *References* to hallucinations, including receiving direct communications or orders.
- *Irrational* or unreasonable demands, solicitations, or claims of being owed something by the target.
- *Obsessive* admiration or affection for the target or efforts to contact or control the target.
- *Inappropriate or suspicious* expression of personal loss, injustice, or desire for revenge. *Information* about potentially violent domestic or personal dispute, in particular the issuance of a protective or restraining order.

Indicators of ideation
- *Inappropriate* display of, or references to, weapons or any other method of inflicting harm.
- *Inappropriate or disturbing* references to, or identification with, death, violence, mass killing, violence in the media, or specific previous violent acts or actors.
- *Expression* of irrational or delusional beliefs, particularly containing violent or paranoid themes.
- *Threats* of physical harm made by any method, whether direct, veiled, or conditional, concerning any target.
- *Nonverbal* threats or threats implied by behavior or pattern of conduct.
- *Any references* to, or failed attempts at, suicide or self-harm.
- *Expressions* of hopelessness or belief that subject has no alternatives to violence.

Indicators of research and planning
- *Any suspicious* activity, such as surveillance, suspicious inquiries, unusual interest in target, or any other untoward attention toward target.
- *Obsessive* interest in the target, including stalking, research, or unusual knowledge or specific information on a person, group, or locale.

Indicators of preparation
- *Evidence* of final act behaviors such as preparing a will, disposing of property, saying goodbye, last rites, fasting, cleansing, confessing, or justifying the threatened act of violence.
- *Obtaining* or preparing weapons, armaments, military-style clothing, methods and attire inspired by prior violent acts, or other well-publicized attack-related materials.
- *Rehearsing*, practicing, or communicating plans and objectives.
- *Recognizing* approaching symbolic dates or events.

Indicators of breach
- *Verbal* or physical abuse, including assault, attempted assault, vandalism, or violent or threatening gestures.
- *Aggressive* or emotional outbursts directed toward a person, group, location, or inanimate objects.
- *Testing* or probing security perimeters or systems.

In addition to the above, report any questionable, untoward, sinister, or otherwise suspect behaviors or contacts.

and schools and religious institutions—are relatively self-contained. The individuals who routinely populate them—the employees, students, worshipers, contractors, and vendors—can be easily identified and educated on the types of behaviors to report and where to direct those reports. Other venues—domestic situations and gathering places such as concerts, fairs, and other collection points—are too amorphous to allow for effective, across-the-board instruction to the public. Training in those venues should focus on the assigned security personnel, including the relevant law enforcement agencies; public service announcements, perimeter controls, such as ticket takers, parking attendants, event vendors; and any other observers or receivers of information from the public, such as 911 communications operators.

Training Within Self-Contained Venues

Training should be provided on the criteria and the DRA approach to occupants of government

facilities directly secured by law enforcement entities. Medical and educational institutions and corporations with in-house policing or security should set up their own DRA processes, as well as training for new employees and periodic refresher training for everyone. Who gets trained should be as broadly conceived as the criteria themselves. Unfortunately, the individuals most in need of training are often the very ones overlooked. They seem hidden in plain sight. At schools, for example, teachers and administrators should receive the training, but so should the bus drivers, crossing guards, groundskeepers, operating engineers, and cafeteria workers. In office buildings, not only the corporate employees but also the engineers, cleaning staff, and snack bar employees should be educated on the criteria and the reporting process. These are the individuals who mingle most with the public and are, therefore, best positioned to overhear or observe behaviors of concern.

Training in Open Venues

In those venues that are not reasonably self-contained, such as shopping complexes and other places the public gathers, the training should include all employees, but also posting of notices, electronic messaging, and other public service announcements alerting visitors on what general behaviors to report. While the entire criteria may be too complex for presentation to the general public, it is essential that the potential receivers of the information are well versed in the details of the criteria. Most sporting arenas these days are flush with electronic signs alerting the attendees on how to text messages to security. That technology should also be used in other public places.

Many established outreach programs, such as "See Something, Say Something" postings, educate the public about the potential for domestic violence, workplace violence, and risks to the public at large (Jenkins & Butterworth, 2018). They offer additional opportunities for introducing the criteria for what information is accepted into established programs. Law enforcement agencies need to ensure that they are prepared to manage reports about disconcerting behaviors regardless of whether a crime has occurred. After receiving an anonymous tip, police in Berkeley, California, began investigating a 16-year-old boy who had tried to enlist others in a plot to shoot up Berkeley High School. While executing a search warrant at the boy's home, police found "assault rifles, knives, and explosives," as well as "electronic items" at his home for use in making more weapons.

Police arrested the suspect on Memorial Day, 2022 (Lukpat, 2022). The case offers an example of how effective detecting, reporting, and acting can be in preventing intended violence.

Organizations also should be ready to accept and evaluate anonymous reports. Doing so may be a departure from past protocol. Nevertheless, it is essential that all reports falling within the adopted criteria be evaluated and appropriate action taken. In practice, this means training 911 communications personnel and others assigned to dealing with the public on the criteria and the agency's DRA process.

Reporting

In addition to training on the organization's criteria, the instruction should also cover the various channels for reporting suspicious behaviors and the designated entity that will receive *and act on* the reported behaviors. That point of contact—and equally trained backup personnel—needs the capability to receive and react to reports day and night, 7 days a week, all year round. Reporting does no good if no one is available to receive or act on the information. In fact, not having the capability to act promptly risks making the situation worse when potential victims or concerned reporters rely detrimentally on the process as a solution to a problem or as an increase in their safety.

The reporting process must include comprehensive methods and portals that are readily available, easily accessible, and operational day and night. They should embrace social media and other technologies to ensure the reporting net spreads as far as possible. In other words, the process should be made as easy and efficient as humanly possible, keeping in mind the continuously evolving communication methods of modern society. Having a hotline style telephone number to call staffed only during regular business hours no longer suffices. Setting up a robust reporting process also creates opportunities to partner with other organizations and jurisdictions to provide more extensive reporting portals and information sharing.

Acting

Receiving a report of an incident or behavior that meets reporting criteria should trigger purposeful actions. This is not to say that every report should prompt an emergency or full-throated response. Rather, every report should be initially evaluated and prioritized according to the potential risk of immediate violence. The initial response should then be calibrated to that evaluation, the first step in acting in response to the report.

We well recognize that not every organization or entity can afford or maintain a threat management unit or full-time designated receiver. For better or worse, local law enforcement, by necessity, fills that need. That is why it seems to us axiomatic that law enforcement is the ultimate default receiver of threat issues and, in critical situations, assumes the role of crisis manager. Incorporating basic threat management training into basic police curricula is the only way to address this problem, which tragically seems to be reaching epidemic proportions.

The second step determines the immediate protective response, such as facility or area lockdowns or protecting individuals, followed by appropriate notifications to other law enforcement agencies, other potential targets, or the public at large. Whoever receives the initial report acts as a clearinghouse. They screen the preliminary reports, prioritize them in order of urgency or importance, collect initial details, issue appropriate notifications, and make relevant referrals. They follow the established protocols as to who on staff should be brought in and what other agencies to contact. For instance, the police department's communications center staffs the point of contact among myriad other duties. When the information comes in, and an immediate law enforcement response is not required, the dispatchers start making notifications to whoever may have the responsibility or is on-call for threat issues as well as the shift supervisor. They also may make appropriate referrals to other affected agencies. Once these preliminary steps are taken, a designated decisionmaker takes over and initiates any law enforcement activities as needed. Only after taking these steps can the traditional threat management process begin, ideally through a team effort or collaborative process.

During this process, every effort should be made to resist any tendency to silo information or take on a "bunker mentality." Sharing all information directly and appropriately with all concerned parties offers the best antidote to bunkers and silos. Pima Community College officials and police solved their disciplinary problems caused by Jared Loughner by suspending him and barring him from campus. No one from the campus, however, alerted surrounding law enforcement jurisdictions or mental health officials about Loughner's erratic behavior and violent musings. By pushing him off campus, they let him loose in the city with only his delusions and fixations for company. On January 8, 2011, Loughner showed up armed at Congresswoman Gabriel Giffords' neighborhood "Congress on Your Corner" meeting with constituents. He killed six people and wounded another dozen, including the congresswoman (Fahrenthold & Williams, 2011).

Similarly, after reviewing all the events leading up to Seung Hui Cho's tragic massacre at Virginia Tech in April 2007, the report of the Virginia Tech Review Panel concluded that "numerous incidents occurred" during Cho's junior year that evinced "clear warnings of mental instability." "Various individuals and departments within the university knew about each of these incidents" but "no one knew all the information and no one connected all the dots" (Mass shootings at Virginia Tech, 2007). One of the greatest risks comes from keeping information within a single unit or organization while the subject crisscrosses jurisdictions or areas of responsibility. Organizations should resist any traditions of handling problems in-house to avoid law enforcement participation or adverse attention. Clear guidelines need to be established on what kind of situations require threat management versus routine discipline or counseling.

Decisions, too, need to be made by those best positioned and qualified to do so. For example, Ethan Crumbley came to the attention of school counselors for what his teachers described as "behavior in the classroom that they felt was concerning" (Rohrlich et al., 2021). Despite that attention, Crumbley killed four and wounded seven others at his school on November 30, 2021. The officials' concerns were not enough to aid them in stopping Crumbley's march down the path to intended violence.

Crumbley's concerning behaviors included a teacher observing him using his cell phone to search for ammunition and another teacher finding on Crumbley's desk a drawing depicting an automatic pistol aimed at the words, "Blood

everywhere." The drawing also included a person with two gunshot wounds atop a laughing emoji. The artwork also included the statements, "My life is useless," and "The world is dead." A school counselor escorted Crumbley to the counselor's office and called Crumbley's parents, summoning them to the school. At the subsequent parental conference, the counselor explained to the Crumbleys that the law required them to get their son into counseling within 48 hr. The parents objected to taking their son out of school that day. Instead, they left, and their son returned to class. The school counselor neither consulted with nor notified any other school officials or law enforcement officers. Nobody addressed the issue of Crumbleys' access to a weapon or exercise the school's authority to search the student's backpack and school locker. Nor did anyone at the school know that the father, accompanied by his son, had recently purchased a semi-automatic pistol, which he stored unlocked in a bedroom drawer. Shortly after returning to class, Ethan Crumbley used that gun to kill four fellow students and wound six others, plus a teacher ("Read the Prosecutor's Account," New York Times, 2021). This was not a student behavior problem to be handled solely by school counselors prioritizing the best interests of the student or the demands of the parents, but a clear risk of potential violence that should have involved an immediate intervention prioritizing the safety of all students, before making a referral to whatever assessment system was available for follow-up.

Threat Management Immediate Response

Effective threat management necessitates responding to reports of some suspicious behaviors with immediate actions by law enforcement, while others may require a more deliberative, team-based process. Designated receivers, upon receiving reports generated by the organization's criteria, should first evaluate the information according to the imminence of the potential violence. As we mentioned above, specialists in the field have designed computer-assisted assessment tools for evaluating potential risks (see Cawood et al., 2020; Cooke & Michie, 2014; Gerbrandij et al., 2018; Hanson et al., 2014; James et al., 2022; Jung & Himmen, 2022; Meloy & Gill, 2016; Storey & Hart, 2014, for a few examples).

The designated receivers should pay particular attention to any behaviors indicative of advanced planning or preparation as these strongly indicate imminent action. As with medical emergencies, suspicious situations can be ranked according to their severity and immediacy for harm. Critical situations require immediate action to stop imminent violence. This involves such measures as immediate protective steps and rapid information gathering focusing on the subject's current whereabouts and capacity for violence. Information on weapon possession, access, or recent acquisition is a priority at this time. Critical situations demand eliminating the subject's ability to do harm. We recognize that a justified immediate response may result in an informed determination that the subject does not pose an immediate threat at that time. In those situations, the subject can be referred if necessary to the appropriate entity for follow-up.

Critical threats are, fortunately, still a rarity. In most situations, the potential for immediate violence or harm remains low. Noncritical events, though no less serious, also need earnest attention, but their potential for violence is not immediate. They loom in the future, such as when the target receives a threatening letter or telephone call and the subject making the threat has no means or ability to carry out the threat. These situations present no apparent risk of present danger on the surface. They still must be attended to, but they carry no urgency or impending risk.

Critical threats require an immediate tactical or investigative response by law enforcement to contain or eliminate the subject's ability to commit violence. Noncritical threats allow for a more deliberative, team-based response employing the full range of threat management strategies. The difference between the responses is one of time. Every report generated by an organization's criteria should prompt an immediate review to ensure no violence hovers imminently, that people are currently safe, and that, in the presence of imminent danger, appropriate security and law enforcement officials act. In other words, the threat manager or the designated receiver should first and immediately determine the imminence of the threat and respond accordingly.

Consider the following two examples:

EXAMPLE 1: An employee, recently terminated from his job, posts photos of various firearms on social media, then starts live streaming his intention to use the weapons to "do some harm" at his appeal hearing that afternoon. Former colleagues of the employee report the postings and the media rant to the company.

EXAMPLE 2: A disgruntled employee evinces sullen and violently angry behaviors around his former colleagues at their local watering hole. His attention, these associates report to the employer, seems focused on his belief that he will soon be terminated because his supervisor is out to get him. Unknown to the employee, his supervisor and personnel officials have already started the process to have him terminated.

Clearly, both examples involve situations posing potential risk. The designated receiver needs to act on both by first determining whether or not either one requires an immediate response. That instant prioritization will then lead to the implementation of protective actions, the appropriate threat management response, and any needed follow-up strategies.

Commonsense helps make the distinction. In the first example, the recently terminated employee shows that he has weapons and is live streaming his intentions. In the second example, the disgruntled employee discusses future actions when any termination proceedings may begin. Both scenarios pose a significant risk of escalation, but the first obviously indicates the risk is far more imminent than the second.

Conclusion

Until the day comes that sufficiently trained and experienced threat managers are out in the field, training as many people as possible within every law enforcement jurisdiction, organization, and threat venue on basic threat concepts, combined with implementing the DRA process, offers the best hope for preventing targeted violence. As with other urgent training programs utilizing aggressive training rollout methods, train-the-trainer courses, webinar seminars, and computer-based learning should be developed. Some private companies offer training in preventing workplace violence, behaviors to watch for, and team coordination. But that training is only for those that can afford the price, and the training itself may vary widely in quality as the field has yet to impose any real quality control. Obviously, fielding more threat managers and establishing more teams promises the optimum way for deflecting the potential for violence, but at present that seems a distant, and not very realistic, goal. The need for trained first responders should continue to be a higher priority for the foreseeable future. Detecting, reporting, and acting offers the best process for recognizing problematic behaviors and bringing them to the attention of those best equipped to respond to them. It also allows for managing those situations that require an immediate tactical or investigative law enforcement response.

Too many times, in too many situations, those handling reports of untoward or sinister behaviors are untrained and inexperienced in dealing with threat scenarios. We have tried in this article to incorporate that reality into our recommendations. The *DRA* process we outlined embraces the reality. It provides for a systematic way to move information about threats and potential violence from those most likely to witness early indicators of it to those best positioned to respond, including during critical emergency situations. By factoring in *time* and *imminence*, the DRA process manages every type of situation, from Nicholas Roske arriving outside Justice Kavanaugh's home to the would-be school shooter blogging his plans on the internet. Adopting reporting criteria based on the concept of the path to intended violence also provides a comprehensible approach to identifying potential subjects embarked on intended violence. When fully integrated, training law enforcement in basic threat management concepts and establishing DRA processes offer a more robust defense against violent targeted attacks.

References

Abdel-Baqui, O. (2022, June 3). Tulsa shooting: Gunman who killed four at hospital had back surgery there in may. *Wall Street Journal*. https://www.wsj.com/articles/gunman-who-killed-four-people-in-tulsa-hospital-had-back-surgery-there-in-may-11654186747?mod=djemalertNEWS

Amman, M., Bowlin, M., Buckles, L., Burton, K. C., Brunell, K. F., Gibson, K. A., Griffin, S. H., Kennedy, K., & Robins, C. J. (ca. 2016). *Making prevention a reality: Identifying, assessing, and managing the threat of targeted attacks*. National Center for the Analysis of Violent Crime. https://www.fbi.gov/file-repository/making-prevention-a-reality.pdf/view

Barnes, S. (2022, January 22). "I will bring every single gun loaded": Virginia mom charged in threat to school over mask policy. *NBC 4 News*. https://www.nbcwashington.com/news/local/i-will-bring-every-single-gun-loaded-virginia-mom-charged-in-threat-to-school-over-mask-policy/2944354/

Bureau of Labor Statistics. (2021). *Occupational employment and wages—Cardiologists*. https://www.bls.gov/oes/current/oes291212.htm

Calhoun, F. S., & Weston, S. (2021). Rethinking the path to intended violence. In J. R. Meloy & J. H.

Hoffman (Eds.), *International handbook of threat assessment* (2nd ed., pp. 392–406). Oxford University Press.

Calhoun, F. S., & Weston, S. W. (2016). *Threat assessment and management strategies: Identifying the howlers and hunters* (2nd ed.). CRC Press. https://doi.org/10.1201/b19689-2

Cawood, J., Scalora, M. & Vinas-Racionero, R. (2020). Comparison of the HCR-20v3, the WAVR-21, v3, and the CAG performance across workplace homicide scenarios: A pilot study. *Journal of Threat Assessment and Management*, *7*(3–4), 200–213. https://doi.org/10.1037/tam0000154

Center for Prevention Programs and Partnerships. (2021). *Threat assessment and management teams*. https://www.dhs.gov/sites/default/files/2021-12/Threat%20Assessment%20and%20Management%20Teams_0.pdf

Centers for Disease Control. (2020). *Leading causes of death*. https://www.cdc.gov/nchs/fastats/leading-causes-of-death.htm

Cooke, D. J., & Michie, C. (2014). The generalizability of the Risk Matrix 2000: On model shrinkage and the misinterpretation of the area under the curve. *Journal of Threat Assessment and Management*, *1*(1), 42–55. https://doi.org/10.1037/tam0000004

Darley, J. M., & Latané, B. (1968). Bystander intervention in emergencies: Diffusion of responsibility. *Journal of Personality and Social Psychology*, *8*(4, Pt. 1), 377–383. https://doi.org/10.1037/h0025589

Fahrenthold, D. A., & Williams, C. (2011, February 26). Tucson shooting suspect Jared Loughner appears to have posted bizarre messages. *Washington Post*. https://www.washingtonpost.com/national-politics/tucson-shooting-suspect-jared-loughner-appears-to-have-posted-bizarre-messages/2011/01/08/AB0xFkD_story.html

Fisher, M., & Keller, J. (2017, November 2). Why does the U.S. have so many mass shootings? Research is clear: Guns. *New York Times*. https://www.nytimes.com/2017/11/07/world/americas/mass-shootings-us-international.html

Gerbrandij, J., Rosenfeld, B., Nijdam-Jones, A. & Galietta, M. (2018). Evaluating risk assessment instruments for intimate partner stalking and intimate partner violence. *Journal of Threat Assessment and Management*, *5*(2) 103–118. https://doi.org/10.1037/tam0000101

Hanson, R., Lunetta, A., Phenix, A., Neeley, J., & Epperson, D. (2014). The field validity of static-99/R sex offender risk assessment tool in California. *Journal of Threat Assessment and Management*, *1*(2), 102–117. https://doi.org/10.1037/tam0000014

James, D. V., Allen, P., Murray, A. W., MacKenzie, R. D., Yang, J., De Silva, A., & Farnham, F. R. (2022). The CTAP, a threat assessment tool for the initial evaluation of concerning or threatening communications: Development and inter-rater reliability. *Journal of Threat Assessment and Management*, *9*(3), 129–152. https://doi.org/10.1037/tam0000173

Jenkins, B. M., & Butterworth, B. R. (2018). *Does "see something, say something" work?* San Jose State University, Mineta Transportation Institute. https://transweb.sjsu.edu/sites/default/files/SP-1118_SeeSomethingSaySomething.pdf

Jenkins, H. W. (2022, May 17). Massacre data arrives a day late. *Wall Street Journal*. https://www.wsj.com/articles/massacre-data-artifical-intelligence-buffalo-shooter-tops-supermarket-payton-gendron-name-11652817738

Jenkins, L. N., & Nickerson, A. B. (2017). Bullying participant roles and gender as predictors of bystander intervention. *Aggressive Behavior*, *43*(3), 281–290. https://doi.org/10.1002/ab.21688

Jung, S., & Himmen, M. K. (2022). A field study on the police use of the Ontario domestic assault risk assessment (ODARA). *Journal of Threat Assessment and Management*, *9*(4), 204–217. https://doi.org/10.1037/tam0000175

Levine, M. (2012). Helping in emergencies: Revisiting Latane and Dareley's bystander studies. In J. R. Smith & S. A. Haslam (Eds.), *Social pyschology: Revisiting the classic studies* (pp. 192–208). Sage Publications.

Lukpat, A. (2022, June 2). A 16-year old boy was arrested for plotting mass shooting, bombing at California high school. *Wall Street Journal*. https://www.wsj.com/articles/a-16-year-old-boy-was-arrested-for-plotting-mass-shooting-bombing-at-california-high-school-11654196055

Mass shootings at Virginia Tech. (2007). *Report of the Virginia Tech review panel presented to Governor Kaine*. Commonwealth of Virginia.

McMahon, P., & Wallman, B. (2018, August 29). How the FBI botched tips about the Parkland school shooter. *South Florida Sun-Sentinel*. https://www.sun-sentinel.com/local/broward/parkland/florida-school-shooting/fl-florida-school-shooting-fbi-tips-problems-20180828-story.html

Meloy, J. R. (2015). Threat assessment: Scholars, operators, our past, our future. *Journal of Threat Assessment and Management*, *2*(3–4), 231–242. https://doi.org/10.1037/tam0000054

Meloy, J. R., & Gill, P. (2016). The lone-actor terrorist and the TRAP-18. *Journal of Threat Assessment and Management*, *3*(1), 37–52. https://doi.org/10.1037/tam0000061

Mosbergen, D. (2022, November 29). Gun death rate nears three-decade high, with men at most risk. *Wall Street Journal*. https://www.wsj.com/articles/gun-death-rate-nears-three-decade-high-with-men-at-most-risk-11669749562

New York Times. (2021, December 3). *Read the prosecutor's account of events before the Michigan school shooting*. https://www.nytimes.com/2021/12/03/us/michigan-prosecutor-crumbley-charges.html

New York Times. (2022, November 24). *A partial list of mass shootings in the United States in 2022*. https://www.nytimes.com/article/mass-shootings-2022.html

Okada, D. (2022, June 20). *Personal e-mail to Weston, S. in author's possession*.

Rohrlich, J., Melendez, P., & Gross, A. (2021, December 2). *Chilling videos, journal found as parents face scrutiny in Michigan school shooting*. https://www.thedailybeast.com/ethan-crumbley-identified-as-oxford-high-school-michigan-mass-shooter?ref=scroll

Storey, J. E., & Hart, S. D. (2014). An examination of the danger assessment as a victim-based risk assessment instrument for lethal intimate partner violence. *Journal of Threat Assessment and Management*, *1*(1), 56–66. https://doi.org/10.1037/tam0000002

Therolf, G. (2019, September 4). The horrific death of Anthony Avalo and the many missed chances to save him. *Los Angeles Times*. https://www.latimes.com/california/story/2019-09-03/anthony-avalos-death-gabriel-fernandez-dcfs-workers

Weston, S. W., & Calhoun, F. S. (2022, January 26). Reporting criteria for detecting violent intent. *Police Chief Online*. https://www.policechiefmagazine.org/reporting-criteria-for-detecting-violent-intent/?ref=0cb0c3c55a63e682a39ff3996a9d262d

Wolfe, J. (2022, June 9). Armed man arrested near supreme court Justice Brett Kavanaugh's home Is charged with attempted murder. *The Wall Street Journal*. https://www.wsj.com/articles/armed-man-arrested-near-supreme-court-justice-brett-kavanaughs-home-high-court-says-11654701203

Received September 8, 2022
Revision received January 4, 2023
Accepted January 18, 2023 ■