9-2024

Operational Components Related to the Development, Implementation, and Sustainability of Behavioral Threat Assessment and Management Programs

Mario J. Scalora

Denise Bulling

NCITE Research Report

Operational Components Related to the Development, Implementation, and Sustainability of Behavioral Threat Assessment and Management Programs

September 2024

RESEARCH TEAM

Members

Mario J Scalora, University of Nebraska Public Policy Center
Denise Bulling, University of Nebraska Public Policy Center

Key Personnel

Andrea Walker, University of Nebraska at Omaha, NCITE
Tin L. Nguyen, University of Nebraska at Omaha, NCITE
Gina Ligon, University of Nebraska at Omaha, NCITE

About NCITE. The National Counterterrorism Innovation, Technology, and Education Center, or NCITE, is a research consortium focused on counterterrorism and targeted violence prevention. It is funded by the U.S. Department of Homeland Security as a Center of Excellence. Based at the University of Nebraska at Omaha, NCITE includes 50+ researchers at partner institutions across the U.S. and Europe.

Acknowledgment. The research in this report was supported by the U.S. Department of Homeland Security (DHS) Science and Technology Directorate (S&T) under Contract Award No. 70RSAT21G00000002/70RSAT23FR0000115.

To cite this report. Scalora, M. & Bulling, D. (2024). *Operational components related to the development, implementation, and sustainability of behavioral threat assessment and management programs*. National Counterterrorism Innovation, Technology, and Education Center.

EXECUTIVE SUMMARY

The purpose of this paper is to summarize the operational components of developing, implementing, and sustaining Behavioral Threat Assessment and Management (BTAM) programs. It explores strategies for gaining support from relevant groups, outlines essential processes and procedures for maintaining BTAM programs, and examines the common challenges in initiating and executing these programs. A successful BTAM program requires planning, effective team management, clear policies, and ongoing support to address and manage potential threats effectively.

BTAM Program Development

Developing a BTAM program requires several initial buy-in considerations, procedural planning activities, team recruitment, education, and reporting infrastructure. Specifically, those looking to establish BTAM programs should:

- Obtain buy-in from key decision-makers and practitioners by aligning BTAM objectives with organizational or community goals
- Define clear policies and the scope of BTAM team activities
- Select members for the BTAM with the appropriate expertise and roles, providing them with ongoing training and education to stay informed about best practices and emerging threats
- Develop operating procedures to ensure consistent, effective operations for reporting behaviors of concern and systematically identifying, assessing, and managing threats

BTAM Program Implementation

The implementation phase includes executing the BTAM program and taking measures to protect individuals and the organization. This involves:

- Taking initial safety steps to protect all relevant parties and prevent any situations from escalating
- Identify available resources for managing persons of concern based on dynamic assessment of the situation
- Thorough documentation of all activities

Sustaining the BTAM Program

To sustain the BTAM program, it is important to cultivate trust and buy-in from both internal and external groups. Additionally, consideration should also be given toward internal risks to sustainability such as:

- Personnel turnover and knowledge management
- Ensuring ongoing support from agency and community leadership
- Process challenges that impede the effectiveness of team BTAM activities

TABLE OF CONTENTS

PREFACE

This report summarizes operational components related to the development, implementation, and sustainability of Behavioral Threat Assessment and Management (BTAM) programs. The information is garnered from the authors' experiences, evolving BTAM practices, and the research literature. It is not a compendium of best practices nor is it an exhaustive literature review. The paper is structured to take the reader chronologically through the evolution of a BTAM program, starting with a description of what BTAM is and is not. Then we delve into operational aspects of developing, implementing, and sustaining a BTAM program. Specific attention is given to methods of obtaining buy-in from relevant internal and external groups (often referred to as "stakeholders"), the processes and procedures required to operationalize BTAM in various settings, and common operational challenges. The authors derived much of this information from lessons learned via prior grant and contract funded community BTAM team development in urban and rural communities.[1] Additionally, the authors had informal discussions with threat assessment experts to clarify and validate the Information presented in this document. No formal research activity was used in the generation of this document. Citations derived from industry and research literature are offered throughout the document. The absence of citations or attribution should lead the reader to assume the recommendation is a product of the authors' experience and validated through informal discussions with a range of BTAM experts.

[1] BJA Award No. 15PBJA-21-GG-04658-STOP; 2020-2022 TVTP Grant awarded to Nebraska Emergency Management Agency; 2023-2025 Contract 104977-O4 Nebraska Department of Health and Human Services; 2018-2023 Nebraska Department of Education Federal Award Identification Number 2018-YS-BX-0113.

INTRODUCTION TO BEHAVIORAL THREAT ASSESSMENT

Behavioral threat assessment is a method of investigating and assessing behaviors of concern, including veiled or direct threats. Behaviors of concern refer to behaviors and related actions that pose a risk to specific individuals, the organization, or both (Fein, Vossekuil, & Holden, 1995). A threat assessment can be the process of choice when someone "feels" threatened or is concerned that a person or group's behavior is potentially escalating toward a violent end.

Threat assessment techniques have been used in a variety of contexts (e.g., corporate organizations, educational institutions, healthcare, law enforcement). The field of threat assessment evolved from practices used to assess and manage dangerousness (potential risk for violence) and represents a blending of behavioral science, intelligence, and law enforcement strategies (Fein & Vossekuil, 1998; 1999).

Traditional violence risk assessment focuses on an individual's propensity for engaging in future violence directed toward unspecified individuals, in unspecified situations, across an unspecified timeframe. In contrast, threat assessment is concerned with assessing the risk of future violence or other undesirable actions (e.g., harassment, sabotage, or disruptive activity) directed toward a specified range of individuals or institutions, in specified situations, sometimes for a specified window of time. The phrase "targeted violence" has been used to describe "situations in which there is an identified (or identifiable) target and an identified (or identifiable) perpetrator" (Fein & Vossekuil, 1998, p. 332). The assumption behind assessing threats related to targeted violence is that it is distinct from other criminal acts, requiring that practitioners engage in analyses that are much different from traditional investigative techniques (Borum et al., 1999).

Three core principles from the behavioral threat assessment approach have been applied to targeted violence (Fein, Vossekuil, & Holden, Jul 1995; Amman et al., 2017).

- First, targeted violence is viewed as a process that takes place over time, during which the subject (person or group posing the threat) must prepare and plan. An attack is the result of a journey laced with problems, difficulties, and conflicts for the subject.
- Second, targeted violence results from the interaction of the subject, a stressful event or activating condition and a setting that does not prevent the violence from occurring. Therefore, attention must be focused not only on the subject but on the surrounding situations.
- The third principle is that successful assessment of targeted violence involves the identification of the subject's continuum of attack-related behaviors (behaviors of concern). Viewing the behaviors of concern on a continuum helps practitioners assess the subject's level and progression of attack planning and preparation.

Behavioral threat assessment (hereafter referred to as threat assessment) is used as a method of disrupting the process of targeted violence, and as a means of identifying the best intervention, treatment, or safety plan to prevent the risk of future threatening behavior. Threat assessment helps determine threat management techniques. Threat management is the process of

monitoring individuals and groups and potentially implementing interventions over time and is an integral part of any threat assessment program (Calhoun & Weston, 2003).

DEVELOPING A BTAM PROGRAM

Several areas should be considered when developing a BTAM program or strategy. More collaborative deliberation during the development phase helps the organization proactively address various challenges that can be anticipated to impact effectiveness and sustainability of future efforts. The structure of BTAM activity is dependent upon the agencies involved as well as the focus of the targeted violence prevention activity. For example, law enforcement agencies hosting BTAM activity protecting public figures and institutions may be less team driven than activity found within educational and corporate settings. Much of this section focuses on various types of organizations, but the lessons can be extrapolated to community teams. Community teams can be thought of broadly as a team of teams attempting to manage difficult community situations. Each organization comes to the table with their own perspective, often as part of the organization's BTAM team.

Planning and Obtaining Decision Maker Buy-in

Many people new to BTAM believe they only need to form and train people to be part of a threat assessment team. While the heart of the BTAM program is the threat assessment process and team activity, a BTAM program or strategy requires more thought and planning. The first step in developing a BTAM program is to get the decision makers of an organization (or in the case of a community-based team, leaders of the community) to buy-in to having a BTAM program.

Selling BTAM to decision makers should include simple, narrow definitions that apply directly to the organization or community. This begins with a champion making a case for BTAM by focusing on the benefits to the organization or community. For example, explain how BTAM will enhance overall safety and that of individual facilities making up the organization, or organizations making up a community team. BTAM is framed as a prevention and a risk management strategy because it facilitates identification of concerning behaviors early and provides an opportunity to prevent harm by lessening the threat through planned intervention and management. BTAM potentially lessens organizational liability when entities can demonstrate they proactively addressed concerns and followed their processes for doing so.

Other benefits relevant to an organization may include how a BTAM program promotes a climate of safety by giving staff and customers positive responses when they encounter a concern. It helps build trust and closer relationships among entities such as human resources, security or safety personnel, mental health partners, management, and others involved in supporting the workforce or customers.

Leadership will want to know the elements that will comprise the BTAM program. For example, before a team can assess concerning behaviors, the organization or community must have a way

to collect and funnel concerns to the team. Before the collection can take place, individuals in the organization or community must know what to look for and how to report it. These and other initial planning considerations should be laid out for decision makers prior to any team development activities. Table 1 contains a list of planning considerations that can be altered to fit the context of the entity forming the BTAM program.

Scope of BTAM Activity

The focus and scope of the proposed BTAM collaboration will dictate the potential membership and types of issues to be addressed. For example, a team may be focused on bridging behavioral health and law enforcement resources to address a subset of concerning contacts toward public officials (e.g., James & Farnam, 2016; Wilson, Pathe, Farnam, & James, 2021). Other BTAM strategies may focus upon specific types of problematic behavior (e.g., stalking) (Pathe et al., 2015). Community-based teams may be developed in response to the need to better coordinate assessment and management of targeted violence across various agencies (e.g., Dreal & Okada, 2021). Bottom line, BTAM teams will not have a "one size fits all" appearance given the goals, resources, and buy-in of various shareholders.

Table 1. **BTAM Program Planning Considerations**

Planning Considerations	
Workplace BTAM policies	What policies need to be in place to: Establish the BTAM program? Establish reporting systems? Guide the BTAM team? Situate BTAM with other processes?
Multiple Reporting Methods	What reporting methods will we use? Anonymous reporting method. Reporting to superior. Other. How will we obtain reports when they go to external entities?
Education of Workforce	How will the BTAM program be explained to staff and customers? How is the workforce educated about what to report? How are supervisors educated about how to receive a report? What to do with the report? How to screen it? How are threat assessment team members trained to receive and act on a report? Manage a concern?
Collaborations	What entities do we need formal agreements with to enact BTAM? (e.g., private security, contractors, Union)

	What entities do we need confidentiality or information sharing agreements with? (e.g., local law enforcement, mental health partners)

Community BTAM teams may be comprised of representatives from organizational BTAM programs, domestic violence professionals, law enforcement, and human service organizations. Similar planning steps are required to form a community team including selling participation in the team to community and organizational leaders. Obtaining buy-in from leaders is easier when BTAM is already part of their organizational culture. Champions for community BTAM should cite benefits to the organization and the community including enhanced safety and improved external relationships.

BTAM Policies

Organizations should incorporate BTAM in their policies and procedures. Policies are overarching and stand the test of time while procedures are more easily altered to reflect updated practices and changing contexts. The policy establishing a BTAM program reflects high level buy in from decision-makers. This sets the stage for all other aspects of team development, reporting processes, and workforce education related to BTAM.

Community BTAM teams function as a collaboration among organizations, often reflecting an intersection among BTAM programs. The "rules" governing how community teams work together on cases can be part of a jointly formed memorandum of understanding (MOU) as opposed to a policy. The MOU is signed by organizational decision-makers who must ensure their organization's participation on the community team is in line with their organizational policies and practices. Healthcare, behavioral healthcare, and educational systems participating on community teams will be looking for ways to collaborate or comment on cases without violating privacy laws (e.g., HIPAA, FERPA). These limits may or may not be part of the MOU but should be recognized in procedures for bringing cases to the community team. For example, cases may be brought to the team without identifying information to help the organization think through potential BTAM interventions or releases obtained before discussing the case with clear limits included in the release delineating the specific type of information that will be disclosed.

Planning: the BTAM Team

Once a decision has been made to move forward with a BTAM program and a policy is in place, a team can be formed and trained. Procedures for the team functioning may be developed ahead of forming the team, or developed by the team after they have more knowledge about BTAM and their role. Each BTAM team must meet operational imperatives within the context of the specific environment (e.g., Cao et al., 2013). The size and make-up of the team will vary depending on the size of the organization, resources available, and assigned authority. Threat assessment and management is an overarching support process and does not replace other services such as employee/workplace violence teams, suicide prevention teams, student focused behavior teams,

workplace safety teams, or other teams focused on specific behavioral areas or populations of concern.

Building a BTAM team requires an approach that is appropriate to the context of the organization, institution, or community (e.g., Dreal & Okada, 2021; James et al., 2010; Pathé et al., 2015; Perloe & Pollard, 2016). Some prefer a very static membership model that is rigidly managed – the same individuals involved with all BTAM activities. Others have found success with a more flexible, layered approach that allows for a base of trained personnel to do an initial assessment of risk factors while having flexibility to bring together a larger team based on the nature of the incident being managed.

The most important objective of the BTAM team, across all contexts, is safety and security. The team needs to be able to respond in a rapid fashion to events as they unfold, in real time. Most of the threat assessment activity should be performed by a small, committed, and accessible team, often referred to as the core team. Smaller organizations or those with fewer resources may not have internal assets with every capability (e.g., investigation expertise, mental health knowledge) and may need to collaborate with external resources to access them when needed.

In general, BTAM teams should include someone with the authority to make safety and security related decisions and allocate direct assets to cover those decisions. If the members on the core team must continually ask for permission to act, they lose the ability to react effectively to the rapidly changing nature of the cases they handle. Threat assessment decisions must be made quickly, often with information gaps.

BTAM team members should establish connections with experienced practitioners on whom they can rely for consultation particularly if team members lack BTAM experience or training. Setting up and utilizing these consultations will provide support for the team as they begin their implementation of the program. These consultation resources will continue to be important even after the members gain sufficient experience to conduct the program on their own. Consultation ensures the best decisions are made at each point of the process.

Beyond the core team, the extended team can be a larger, multi-disciplinary body composed of members from across the organization. This extended team should meet regularly to discuss current cases, introduce new cases, and possible emerging cases or situations. When there are no ongoing cases to discuss, the team can use the regularly scheduled time to revisit procedures, test their operating assumptions based on other cases (e.g., taking known cases from the news and doing a simulation or tabletop exercise about how the team would handle it if were to occur in their organization.)

The members of the extended team bring a substantially different mix of skills, knowledge, and experience to the BTAM program than those on the core team. The core team is primarily focused on threat investigation, mitigation, and initial intervention implementation. The extended team is a multifaceted group concerned with the continued management of threat cases and courses of action that will be most beneficial to all of those concerned. The larger team may include

representatives from different parts of the organization (management, human resources, employee assistance programs, legal counsel, communications, etc.).

The extended team members could be called upon outside of a regular meeting by the core team to help inform assessments or interventions specific to that member's responsibilities. While the core team is responsible for safety and security, implementation of the interventions is often better handled through other entities such as human resources. This layered approach to handling threats (core and extended teams) provides an apparatus for rapid response and allows oversight and coordination at another level to help guide interventions.

Organizations may require or request their workforce members to participate on BTAM teams. Some organizations rely heavily on external partners to be part of their team (e.g., law enforcement, mental health). Obtaining buy-in from potential BTAM team members should begin with the organization citing benefits of participating such as personal growth and development, contributing to workplace or community safety, and confidentially assisting co-workers, customers, and/or community members. Note that the organization is investing in their training and participation on the team as part of the organization's safety strategy.

Recruitment of BTAM team members is ongoing because of the turnover in an organization. Current BTAM team members can be ambassadors for the program and a resource to provide realistic feedback to potential team members about the time commitment, benefits, and challenges associated with being part of the team. This is true for organization and community BTAM teams.

Education: the BTAM Team

Once BTAM team members are identified, they should receive education about the basics of threat assessment, what it means to be on a team, what the team does, how to screen reports, and how to assess and manage potential threats. Training should be delivered in stages and not be considered an initial solitary event as team members will vary both in their acquisition of knowledge and their ability to apply that knowledge to actual scenarios. Further, even experienced teams can benefit from continuing education to raise skills and enhance team functioning. Ideally, the team will receive ongoing education and training to deepen their knowledge of BTAM as they become more aware of the intricacies involved with assessing and managing cases.

Operationally, education for the team must precede educating the rest of the workforce or the community about what and how to report. This ensures team members know what to do when reports start coming to them. The scope of this document does not include a full review of what should be included in educating the BTAM team members, however, BTAM team training should begin with an overview of the fundamental principles upon which BTAM is based. Case examples interspersed in the training will move the team toward a better understanding of their role and the resources required to fulfill their charge. Fundamentals may also include a review of the organization's policies (and/or community team agreements) and expectations for

documentation, team availability and organization, and the limits of their authority to act or intervene

Planning: BTAM Team Operating Procedures

Once the BTAM program policy is in place and the team members are trained, ensure that initial procedures are drafted. These procedures can be altered after they are tested by the team. Procedures should address the following:

- Frequency of BTAM extended and core team meetings.
- Who receives and screens reports.
- Who has authority to call the full team together outside of regular meetings.
- How the core team will operate (who leads the team, who steps in to lead when that person is not available, under what circumstances extended team members will be brought into the discussion, how team activities are documented, managing confidentiality and conflicts of interest, etc.).
- How to activate resources for assessment or management interventions.
- Activating emergency resources and protecting potential targets.
- Documentation practices.

Procedures for the BTAM program can be brief but should provide enough detail to guide the actions of team members. There should be an easy mechanism to alter procedures after the team has some experience assessing and managing threats. After training, BTAM team members will likely identify new procedures to develop and may need to change procedures that are not realistic or plausible given the team's authority and resources. New partnerships may also give rise to altered procedures. For example, a team may have a member of an employee assistance program (EAP) as a core member but decide later to have a different mental health professional on the core team instead because EAP often has conflicts of interest with the personnel they serve.

The BTAM program can never promise an outcome but can promise fidelity to a process or approach to assessing and managing threats. The policies, procedures, and training are the process guides and form the backbone of the BTAM program. BTAM teams will always face challenges related to the levels of available information as well as resources to support assessment and management efforts.

Reporting Behaviors or Concerns

Once the team is trained and procedures are in place, they are ready to accept reports. However, staff and customers must first be made aware of what to report and how to report it. The educational component supporting reporting must be repeated regularly to ensure reporting is normalized and accepted.

Reporting should be accessible to all through multiple means. Some individuals will feel more comfortable with anonymous reporting while others will want to talk to a live person who can advise and assist them (Low, Scalora, Bulling, DeKraai, & Siddoway, 2024). There may be

organizational constraints or policies that affect reporting. These policies must be considered and incorporated into the plan for reporting concerning behaviors.

Obtaining the buy-in from workforce members and customers (or community members) requires three messages.

- First, describe the overall BTAM program emphasizing its role in proactively keeping everyone safe.
- Second, describe how reports are managed, and the confidentiality associated with reporting. Most BTAM programs also include a caveat about the consequences of making false reports.
- Third, describe the multiple ways someone can make a report. This should include at least one method of reporting anonymously such as a tip line or digital reporting portal.

The authors learned through a previous project that various community shareholders may prefer to reach out to groups or representatives they may have more trust in (e.g., community service providers, educators, cultural or faith group representatives) rather than law enforcement or security mechanisms. BTAM reporting efforts should include education of people in these informal channels about what to do with reports of concerning behavior.

Research supports the importance of anonymous reporting especially for groups who have or perceive they have less power or status in an organization or community (Low et al., 2024). Some people will take their concerns to supervisory personnel or trusted coworkers. These report-takers should receive training about what to do when they receive a report about concerning behaviors. Not all reports will get to the BTAM team because they may be managed at a lower level (e.g., by supervisors or the person receiving a report). Supervisors and those in positions to receive reports (e.g., teachers, trusted community members) should be given guidelines about what behaviors of concern may require additional follow-up with the BTAM team.

In general, the following are often cited as examples of what to report.

- Anything that raises suspicion or concern.
- Contacts (e.g., letters, email, phone, voice mail, face to face visit) that make negative reference to an organization or community member, even if they don't make a threat.
- Any contacts that contain a threat (overt or implied), regardless of method used.
- Subject displays agitated and disruptive behavior (regardless of whether a threat is made).
- Harassing or following behavior (including phone calls, emails, text messages, physical approach or following).
- Subject displays signs of serious mental illness and engages in problematic contact behavior.
- Behaviors suggestive of stalking.

Additional behaviors can be added to this list, but we recommend keeping the list broad to encompass the many ways concerning behavior can be manifested.

Implementation of BTAM

The first concern in the BTAM process is always safety. Does the initial report of the behavior(s) of concern warrant immediate intervention or is there time for a more thorough assessment? The second consideration is gathering complete information to create an intervention and management strategy. Finally, the team must place the available information in context, to determine an appropriate and feasible intervention strategy.

Initial Safety Steps

The person receiving the initial report begins by determining whether preliminary safety plans must be initiated. This decision is based on the nature and seriousness of the case, the appearance of established behavioral indicators and the totality of the circumstances. The most immediate concern is the identification of the target and determining the threat posed to that target by the subject. If the threat of harm is imminent, the case will likely become a traditional law enforcement intervention, rather than a threat assessment. However, if the threat is not imminent, but there are indications of risk of violence, a threat assessment case may be opened.

Tracking motivation across time will provide valuable information regarding the subject. If the subject is often changing motivation for communications, this is indicative of something very different than if the subject is stuck on one topic and communicates frequently and intensely about it. Tracking the intensity of the contact behavior across time gives the assessor information about their current state. If the intensity is escalating, for example using all capital letters or more profane language, it can indicate that the subject is becoming increasingly agitated and may be closer to acting on a threat action. The following aspects should be examined and tracked:

- Have there been multiple prior contacts or multiple methods of contact?
- Are the contact behaviors escalating in intensity, language, or frequency?
- What is the nature of threatening language?
- Has there been surveillance or stalking-like behavior?
- Has there been intrusive harassment toward the target?
- Has there been attempted contact across multiple settings?
- Has there been attempted contact with multiple targets?
- Have there been any demands made?

Threat Assessment Interventions

The interventions required to manage a specific threat case will vary according to the nature of the case, available information, and available resources. Interventions should always be selected with safety in mind. However, this consideration should be tempered by the intrusiveness of the interventions with the least intrusive intervention that will ensure safety selected. A threat to implementation of BTAM interventions is the myth that harsher options are more effective than less intrusive ones. An underlying value in threat assessment and management is to treat subjects with respect and dignity. Interventions based on this principle may be less harsh but more effective in lessening the threat. For example, an organization may decide an employee needs to

be separated or terminated, but a “soft landing” that allows the person to depart with dignity or even some benefits in place may lessen the overall threat to the organization or target. BTAM endeavors may be viewed with skepticism or concern by some people within a community, company or workplace if it is perceived that the BTAM approaches tend to be punitive or harsh. Such a perception might also negatively impact reporting (Hodges, Low, Viñas-Racionero, Hollister & Scalora, 2016).

Threat management as dictated by the context of BTAM efforts (e.g., community, education, workplace) require different levels and kinds of resources to develop and sustain collaborative efforts. Investigative and threat assessment activities, especially within law-enforcement and protective agency contexts (e.g., James, Kerrigan, Forfar, Farnham, & Preston, 2010; Scalora, Hawthorne, Pellicane, & Schoeneman, 2020; Scalora & Zimmerman, 2015) can be performed by core staff with the proper training (e.g., law enforcement, mental health). However, the range of management strategies that might be suggested by the assessment often require collaborative relationships and partnerships that may span agency and other community boundaries (Cao, Ramirez, & Peek-Asa, 2013; Dreal & Okada, 2021; Calhoun & Weston, 2016; James, Kerrigan, Forfar, Farnham, & Preston, 2010). Such management and intervention strategies may range from unobtrusive (e.g., file and monitor, family engagement, mental health referral) to more restrictive (e.g., civil restrictions, mental health commitment, criminal filing) (Calhoun & Weston, 2016). Teams choose a management approach based upon the pros and cons of given strategies, practical concerns related to resource availability, and relevant legal considerations. Agencies may also vary in their willingness to share critical information given concerns related to confidentiality or other barriers to information sharing (e.g., HIPAA, FERPA).

A critical aspect of team engagement related to threat management involves which persons, agency and resources might be best suited to facilitate the engagement of the persons of concern who are the focus of the threat assessment. In addition to the communication issues necessary with case collaboration and management, there is often a need to access properly trained practitioners (e.g., behavioral health, social services) who are willing to address potentially high-risk behavior. Threat management efforts often focus on enhancing the motivation of the person of concern to de-escalate the problematic behavior. Punitive or confrontive approaches may amplify the already existing grievances at the base of the concerning behaviors.

Management of the expectations of community members and targeted parties requires resources and expertise over and above the investigative and assessment resources. Even if the behaviors of concern are deemed to be of low concern for violence, the targeted parties may legitimately feel concerned for their safety and demand a potentially strong response. Further, targeted parties may require and benefit from advocacy services coordinated with BTAM efforts to enhance safety planning as well as maintain continued contact to monitor behavior and address concerns.

Individuals and groups surrounding the contexts of the concerning behavior (e.g., co-workers, community members) may also share heightened concerns based upon exposure to the

behaviors of concern either directly (witnessing physically or online) or indirectly (e.g., via gossip, third party communications). Development of legally supported communication strategies may require the expertise of various legal and communication practitioners, for example.

Documentation

Threat assessment case reports should be thorough and detailed. Each entry to the report should be dated with detailed information regarding the case, including but not limited to:

- Nature of the concerning behavior.
- Date the report was received.
- Types/dates of contacts.
- Content of contacts.
- Known risk and protective factors.
- Level of concern and what it is based on.
- Interventions or actions that were taken.
- People involved in the investigation and interventions.
- Any outcomes resulting from the interventions or actions.

Sustaining a BTAM Program

A range of considerations were noted concerning the development of BTAM efforts that, by implication, also have significant relationships to the sustainability of BTAM collaborations.

Need for Cultivating Trust & Buy-in: Internal and External Groups

A critical lesson learned involves the need to both obtain and subsequently maintain buy–in from key sectors both internally and externally. There is a substantial need to recognize the interests of various groups, including: the public, persons who are targeted/threatened/harassed, employers/Institutions, and the persons of concern.

Substantial effort is required to build trust with key stakeholders within an organization, their customers, and members of the public. Community buy-in is dependent upon the way threat assessment and other safety activity is marketed to and used within a community.

- Successful implementation of a preventive/public health approach to targeted violence prevention in local communities requires enlisting local partners who are interested in applying this approach (e.g., Wilkins, Tsao, Hertz, Davis & Klevens, 2014). Engage partners in key community functions related to threat assessment (e.g., advocacy, volunteerism, service delivery, education, law enforcement).
- Community service providers are often closest to individuals in the community affected by violence but may or may not be trusted. Practitioners cannot assume that levels of trust were pre-established within communities. Violence prevention and safety strategies can be hampered by previous conflicts and misunderstandings related to prior events within parts of a community. Understanding the preconceptions groups bring to the table is critical to implementing and maintaining threat assessment strategies.
- Highlight the values of prevention, dignity and respect given apprehensions that exist among groups regarding how violence prevention programming is both perceived and

implemented. Highlight that a key aspect of threat assessment is to de-escalate problems early rather than waiting for the need to engage in more restrictive consequences.

- Feature prevention as a key focus noting that efforts will be made in providing assistance and de-escalating tensions. Even use of the terminology "threat" assessment may suggest to some that the focus is strictly upon catching someone in negative behavior versus de-escalation.
- Educate people about the violence prevention process. Emphasize what happens after a report is made. They may be reticent to participate if the perception of harsh consequences prevails.
- Address barriers to reporting. Research has shown that people choose not to report concerning behavior for several reasons: lack of trust in the process or organization; personal risk; not wanting to get involved; unsure of what or how to report; concern about not being taken seriously; or language barriers (Low et al., 2024; Hodges et al., 2016). Education is one way to address these barriers but may not be the only way to do so. Organizations and communities should assess what the barriers are for their constituents and tailor their choice of reporting mechanisms and educational content to directly address them. For example, marketing reporting to address concerns about not wanting to get involved may include an emphasis on the shared responsibility for safety highlighting how the process emphasizes dignity and respect for everyone.

Internal Risks to Sustaining TA Teams and Activities

Challenges for implementing and sustaining threat assessment teams vary but generally can be viewed as occurring in three areas: personnel, resource, and process challenges.

Personnel Challenges/Turnover

Several challenges are related to personnel or workforce issues. The first challenge is turnover in BTAM team membership. Each time a new person comes into a BTAM team they must be trained in fundamentals and organizational practices. Additionally, some team members may not be very active on the team and require refresher training. Without ongoing training, the team is unlikely to maintain fidelity to the BTAM process. Remember, the BTAM program cannot promise an outcome, but can promise fidelity to a process based on the policies, procedures, and the training.

The second workforce challenge involves personnel changes throughout partner organizations. As people are promoted, they take on more responsibility for receiving reports from those under them. New supervisory personnel should receive education about their responsibility to screen reports while other supervisory personnel continually refresh their training. Personnel changes or additions threaten overall reporting consistency if the organization or community does not routinely provide education about the BTAM program, reporting structures, how and what to report, and the benefits of reporting to all workforce members.

Agency and Community Leadership Support

Challenges may occur when leadership changes or support from leadership dwindles. This can lead to fewer resources dedicated to the BTAM program and potentially an erosion of support

needed to sustain it. Keeping leadership informed of BTAM activities and periodically revisiting the benefits of the program may be necessary. Having a leadership representative on the extended BTAM team may help with this challenge by creating a direct link to decision makers.

An additional leadership challenge is that leaders and other interested people may demand more harsh responses to targeted violence within a community. Such demands may often occur in response to either a rather public or disturbing situation (e.g., disruptive internet threatening post) that may have a range of people bothered and demanding a strict response.

Process Challenges

There are several process challenges to sustaining a BTAM program. First, there is a need to recognize that TA is hard work. There are a range of psychological and physical reactions practitioners can encounter because of assessing and managing various aspects of targeted violence (Kim, Chesworth, Franchino-Olsen & Macy, 2022). Caring for the psychological and physical manifestations of this work in practitioners, both traumatic and otherwise, requires a concerted effort.

Another potential challenge to the process is an overreliance on tools. Threat assessment and management as a process is iterative and there is no single checklist or instrument that works in every situation. Relying on a single tool may blind the BTAM team to emerging threats that are not included in the tool. A guideline approach requires BTAM team members to use their judgement along with any tools that are appropriate to the context and population. The authors strongly recommend a guideline approach and avoiding rigid models using checklists and forms to determine level of risk. This strategy does not exclude the use of instruments and draws upon the current research literature that guides rather than dictates risk levels and interventions.

The team should contemporaneously document how decisions are made (e.g., what is considered, what information is available). The documentation should tell the story of what interventions were implemented, how or if they worked as intended, and how the team adhered to or veered from their BTAM process.

A process challenge sometimes encountered by teams is the lack of consultation resources to help the team address difficult case situations as well as revisit team processes. As collaborators implement threat assessment teams, it may be challenging to find or accept mentoring from experienced threat assessment and management professionals. Having content experts available for local training and consultation is essential for effective team functioning.

A persistent process challenge is related to common misperceptions about privacy laws. This can interfere with reporting, managing cases over time, and getting pertinent information about threats from other entities. Two specific privacy laws are subject to misunderstanding by professionals and the public: the Federal Educational Rights and Privacy Act (FERPA) and the Health Insurance Portability and Accountability Act of 1996 (HIPAA). There is often a broad misunderstanding of what information these laws allow or prohibit one from disclosing. What

makes matters worse is that the two laws often conflict in what circumstances warrant what amount of information that can be shared.

FERPA is a United States Federal Law that was originally enacted in 1974 (See 10 U.S.C. § 1232g; 34 CFR Part 99). It is intended to protect the privacy of students' "education records," and personally identifiable information from those records, at any educational agency or institution that receives funding from the U.S. Department of Education without a parent or eligible student's written consent. Only student "education records" fall under FERPA, which means observations and conversations do not apply to the privacy law. Records from medical and psychological treatment, also known as "treatment records," are not considered "education records" if they are maintained by the institution and used only in connection with the student's treatment (See 34 CFR § 99.3). In addition, FERPA does not apply to records created by law enforcement agencies serving in educational settings.

HIPAA was enacted in 1996 to protect individually identifiable health information by setting privacy standards and safeguards (See 45 CFR Parts 160, 162, and 164). There are two main parts to HIPAA: the Administrative Simplification provisions and the additional rules issued by the U.S. Department of Health and Human Services, which include Security and Privacy rules. Neither HIPAA nor FERPA prevents sharing information when there is an emergency, or if the information could protect the health or safety of the individual or others. BTAM team members should be familiar with the exceptions to both laws.

Finally, creating mechanisms for data collection and management to facilitate accountability is valuable given the various apprehensions that can arise related to BTAM activities (Scalora & Racionero, 2021). For example, leadership may question the effectiveness of threat assessment and management efforts when contemplating resource allocation during budgeting. Various groups might raise questions about whether investigative or intervention efforts are having disproportionate negative impacts upon certain populations or question the quality of threat assessment efforts (e.g., Goodrum, Evans, Thompson & Woodward, 2019). Having mechanisms to track BTAM team efforts facilitates quality assurance activity to evaluate team practices and outcomes and answer external questions as they arise.

References

Amman, M., Bowlin, M., Buckles, L., Burton, K.C., Brunell, K.F., Gibson, K.A., Griffin, S.H., Kennedy, K., & Robins, C.J. (2017). Making Prevention a Reality: Identifying, Assessing, and Managing the Threat of Targeted Attacks, Washington, D.C.: Federal Bureau of Investigation, National Center for the Analysis of Violent Crime, Behavioral Analysis Unit.

Borum, R., Fein, R., Vossekuil, B., & Berglund, J. (1999). Threat assessment: Defining an approach for evaluating risk of targeted violence. Behavioral Sciences and the Law, 17, 323-337.

Calhoun, F.S. & Weston, S.W. (2003). Contemporary threat management: A guide for identifying, assessing, and managing individuals of violent intent. San Diego, CA: Specialized Training Services.

Calhoun, F.S., & Weston J.D., S.W. (2016). Threat Assessment and Management Strategies: Identifying the Howlers and Hunters, Second Edition (2nd ed.). Routledge. https://doi.org/10.1201/b19689

Cao, Y., Yang, J., Ramirez, M., & Peek-Asa, C. (2013). Characteristics of workplace threats requiring response from a university threat assessment team. Journal of Occupational and Environmental Medicine, 55(1), 45–51. ttps://doi.org/10.1097/JOM.0b013e31826bb66a

Dreal, J. V., & Okada, D. (2021). A review of the working dynamics of the Salem-Keizer/Cascade Student Threat Assessment and Willamette Valley Adult Threat Advisory Team models. In J. R. Meloy & J. Hoffmann (Eds.), International handbook of threat assessment (2nd ed., pp. 654–668). Oxford University Press. https://doi.org/10.1093/med-psych/9780190940164.003.0036

Fein, R. A., Vossekuil, B., & Holden, G. A. (Jul 1995). Threat Assessment: An Approach To Prevent Targeted Violence. Research in Action, 1-8. https://doi.org/10.1037/e517592006-001

Fein, R. A., & Vossekuil, B. (1998). Preventing attacks on public officials and public figures: A Secret Service perspective. In J. R. Meloy (Ed.), The psychology of stalking: Clinical and forensic perspectives (pp. 175–191). San Diego, CA: Academic Press.

Fein, R. A., & Vossekuil, B. (1999). Assassination in the United States: An operational study of recent assassins, attackers, and near-lethal approachers. Journal of Forensic Sciences, 44, 321–333. https://doi.org/10.1520/JFS14457J

Goodrum, S., Evans, M. K., Thompson, A. J., & Woodward, W. (2019). Learning from a failure in threat assessment: 11 questions and not enough answers. Behavioral Sciences & the Law, 37(4), 353–371. https://doi.org/10.1002/bsl.2399

Hodges, H. J., Low, E. C., Viñas-Racionero, M. R., Hollister, B. A., & Scalora, M. J. (2016). Examining the reasons for student responses to threatening behaviors on a college campus. Journal

of Threat Assessment and Management, 3(3-4), 129–142. https://doi.org/10.1037/tam0000063

James, D. V., & Farnham, F. R. (2016). Outcome and efficacy of interventions by a public figure threat assessment and management unit: A mirrored study of concerning behaviors and police contacts before and after intervention. Behavioral Sciences & the Law, 34(5), 660–680. https://doi.org/10.1002/bsl.2255

James, D. V., Kerrigan, T. R., Forfar, R., Farnham, F. R., & Preston, L. F. (2010). The fixated threat assessment centre: Preventing harm and facilitating care. Journal of Forensic Psychiatry & Psychology, 21(4), 521–536. https://doi.org/10.1080/14789941003596981

Kim J, Chesworth B, Franchino-Olsen H, Macy RJ. (2022) A Scoping Review of Vicarious Trauma Interventions for Service Providers Working with People Who Have Experienced Traumatic Events. Trauma Violence Abuse, 5,1437-1460. doi: 10.1177/1524838021991310. Epub 2021 Mar 9. PMID: 33685294; PMCID: PMC8426417.

Low, E. C., Scalora, M. J., Bulling, D. J., DeKraai, M. B., & Siddoway, K. R. (2024). Willingness to report in military workplace violence scenarios: Initial findings from the Marine Corps on the impact of rank and relationship to the person of concern. Journal of Threat Assessment and Management, 11(1), 19–31. https://doi.org/10.1037/tam0000202

Pathé, M. T., Lowry, T., Haworth, D. J., Webster, D. M., Mulder, M. J., Winterbourne, P., & Briggs, C. J. (2015). Assessing and managing the threat posed by fixated persons in Australia. Journal of Forensic Psychiatry & Psychology, 26(4), 425–438. https://doi.org/10.1080/14789949.2015.1037332

Perloe, A., & Pollard, J. W. (2016). University counseling centers' role in campus threat assessment and management. Journal of Threat Assessment and Management, 3(1), 1–20. https://doi.org/10.1037/tam0000051

Scalora, M. J., Hawthorne, D., Pellicane, T., & Schoeneman, K. (2020). A glimpse of threat assessment and management activity performed by the United States Marshals Service. Journal of Threat Assessment and Management, 7(1-2), 85–97. https://doi.org/10.1037/tam0000149

Scalora, M. J., & Racionero, R. V. (2021). Successful development of threat assessment and management programming within a Midwestern university. In K. Heilbrun, H. J. Wright II, C. Giallella, & D. DeMatteo (Eds.), University and public behavioral health organization collaboration: Models for success in justice contexts (pp. 107–124). Oxford University Press. https://doi.org/10.1093/medpsych/9780190052850.003.0007

Scalora, M. J., & Zimmerman, W. (2015). Then and now: Tracking a federal agency's threat assessment activity through two decades with an eye toward the future. Journal of Threat Assessment and Management, 2(3-4), 268–274. https://doi.org/10.1037/tam0000057

Wilkins, N., Tsao, B., Hertz, M., Davis, R., Klevens, J. (2014). Connecting the Dots: An Overview of the Links Among Multiple Forms of Violence. Atlanta, GA: National Center for Injury Prevention and Control, Centers for Disease Control and Prevention Oakland, CA: Prevention Institute.

Wilson, S. P., Pathé, M. T., Farnham, F. R., & James, D. V. (2021). The fixated threat assessment centers: The joint policing and psychiatric approach to risk assessment and management in cases of public figure threat and lone actor grievance-fueled violence. In J. R. Meloy & J. Hoffmann (Eds.), International handbook of threat assessment (2nd ed., pp. 471–487). Oxford University Press. https://doi.org/10.1093/med-psych/9780190940164.003.0027