PREVENTING TARGETED WORKPLACE VIOLENCE

A U.S. SECRET SERVICE GUIDE TO BEHAVIORAL THREAT ASSESSMENT AND MANAGEMENT

U.S. DEPARTMENT OF HOMELAND SECURITY
UNITED STATES SECRET SERVICE
NATIONAL THREAT ASSESSMENT CENTER

This publication is in the public domain. Authorization to copy and distribute this publication in whole or in part is granted. However, the U.S. Secret Service star insignia may not be otherwise reproduced or used in any other manner without advance written permission from the agency. While permission to reprint this publication is not necessary, when quoting, paraphrasing, or otherwise referring to this report, the citation should be: **National Threat Assessment Center. (2026). *Preventing Targeted Workplace Violence: A U.S. Secret Service Guide to Behavioral Threat Assessment and Management*. U.S. Secret Service, Department of Homeland Security.**

MESSAGE FROM THE CHIEF

Workplace violence is a significant and persistent challenge, harming tens of thousands of people and impacting numerous organizations and communities across the nation each year. Some of the most severe acts of workplace violence are premeditated attacks targeting the places where we routinely work and visit, including offices, restaurants, hospitals, hotels, schools, factories, and many others. The consequences of these acts of targeted workplace violence are devastating to our nation, resulting in trauma, injury, and most tragically, loss of life.

For over 25 years, the U.S. Secret Service National Threat Assessment Center (NTAC) has examined targeted violence and published groundbreaking research and operational guidance to support community violence prevention efforts. This support continues with the release of ***Preventing Targeted Workplace Violence: A U.S. Secret Service Guide to Behavioral Threat Assessment and Management***, which combines key findings from NTAC's research on mass attacks impacting workplaces with our latest operational guidance to assist organizations in implementing behavioral threat assessment and management programs as part of their overall violence prevention strategies.

Preventing targeted violence in our workplaces requires a team approach, and NTAC stands ready to provide continued support to our organizational partners as they implement targeted violence prevention programs. With the creation and distribution of this publication, we offer a blueprint to support agencies, organizations, and other workplaces as they work tirelessly to ensure the safety of their workforce and the general public.

Dr. Lina Alathari
Chief, National Threat Assessment Center

TABLE OF CONTENTS

Key Terms 7

Introduction 8

Part 1: Mass Attacks at Workplaces 11

The Incidents 13

Impact 13

Weapons Usage 13

Resolution 14

The Attackers 15

Demographics 15

Stressors 15

Elicited Concern 16

Criminal History 16

Affiliation to Targeted Location 17

Current or Former Employees 18

Customers, Clients, Patients, and Visitors 23

Romantic Partners and Relatives 25

Mental Health Symptoms Across Attacker Types 26

Research Conclusion 27

TABLE OF CONTENTS

Part 2: A Guide for Workplace Violence Prevention 29

Step 1: Commit to Employee Safety and Support 33

Secure Leadership Buy-In 34

Offer Resources and Guidance to Employees 35

Promote Internal Collaboration 36

Build Community Partnerships 38

Step 2: Establish BTAM Program Policy and Procedures 40

Establish Policy 40

Develop Standard Operating Procedures (SOPs) 42

Continuous Improvement 43

Step 3: Assemble a Multidisciplinary BTAM Team 44

Determine BTAM Team Composition 45

Train BTAM Team Members 48

Establish Regular BTAM Team Meetings 49

Step 4: Identify and Process Reports of Concerning Behavior 50

Recognize Behaviors of Concern 50

Implement a Bystander Reporting Program 55

Process and Triage Reports 57

TABLE OF CONTENTS

Step 5: Gather Information to Assess for Risk 59

Preliminary Inquiry vs. Full Assessment 62

The Systems Approach 62

Assessment Themes 67

Make an Assessment of Risk 74

Step 6: Develop Risk Management Strategies 75

Phases of Risk Management 75

Elements of Effective Risk Management 76

Risk Management Strategies 79

Step 7: Promote a Safe and Supportive Organizational Climate 86

Strategies to Promote a Safe Climate 87

Step 8: Provide Training for All Employees 89

Availability and Accessibility 89

Content 90

Frequency 90

Continuous Messaging 91

Conclusion 92

Appendices 94

Endnotes 97

KEY TERMS

Targeted Workplace Violence: A premeditated act of violence perpetrated at a workplace, directed at a specific individual, group, or location, regardless of motivation and generally unrelated to other criminal activity.

Known or Knowable: An individual is *known or knowable* when their identity, affiliation, or patterns of behavior are either already recognized (i.e., known) or can reasonably be identified (i.e., knowable) based upon their frequent or substantive contact with the workplace. Common types of individuals that are known or knowable to a workplace include current or former employees; regular or notable customers, clients, patients, or visitors; and the current or former romantic partners or relatives of individuals connected to the organization.

Behavioral Threat Assessment and Management (BTAM): A behavior-based approach to proactively prevent incidents of targeted violence. The U.S. Secret Service behavioral threat assessment model was developed to *identify* individuals displaying threatening or concerning behavior, gather information to *assess* if an individual poses a risk of violence, and then *manage* the risk by implementing appropriate interventions.

Individual of Concern: Any individual who has exhibited concerning behaviors that may indicate a potential risk of harm to themselves or others in the workplace setting.

Concerning Behavior: Actions or communications by an individual that are objectively or contextually troubling or inappropriate and indicate a potential risk of violence.

Systems Approach: A process of gathering information from various community systems in order to provide a comprehensive and reliable assessment of an individual's thinking and behavior.

Assessment Themes: Areas of inquiry that, when explored, will provide a contextual understanding of an individual's mindset, behavior, and circumstances that will allow a BTAM team to assess if the individual poses a risk of violence.

Risk Management: The strategies and efforts pursued by a BTAM team with the goal of making a violent outcome less likely. Risk management should always be driven by the results of the behavioral threat assessment.

INTRODUCTION

NTAC's mission to prevent targeted violence involves the publication of research and guidance for our public safety partners across the United States, with further support offered through our training and consultation missions. Targeted violence encompasses multiple forms of violence that have impacted communities across the nation, including attacks targeting government officials, schools, houses of worship, and workplaces.

Over two decades of NTAC research has continually affirmed that targeted violence can be prevented when communities are equipped with the knowledge and resources to recognize the warning signs and intervene. In 2023, NTAC published ***Mass Attacks in Public Spaces: 2016 – 2020***,[1] a report that examined 173 acts of mass violence perpetrated in public and semi-public spaces across the United States over a five-year period. One key finding from the study was that **businesses were the most frequent type of location impacted by acts of mass violence**, including restaurants, bars, banks, office spaces, warehouses, and hospitals. To further understand the scope of attacks impacting this sector, NTAC developed a project specifically aimed at understanding and preventing targeted acts of violence within workplace settings. This publication presents research and guidance on preventing targeted workplace violence to support organizational safety stakeholders in a variety of professional roles, including those responsible for management, security, human resources, information technology, cybersecurity, and insider threat. It is also intended for individuals with broader public safety responsibility, including state and local law enforcement, mental health professionals, and other community partners.

THIS PUBLICATION IS INTENDED TO ASSIST...

This publication offers key research findings and operational guidance for preventing acts of targeted workplace violence. ***Targeted workplace violence*** can be defined as a premeditated act of violence perpetrated at a workplace, directed at a specific individual, group, or location, regardless of motivation and generally unrelated to other criminal activity. NTAC research on targeted violence has continuously found the following:

TARGETED WORKPLACE VIOLENCE:

A premeditated act of violence perpetrated at a workplace, directed at a specific individual, group, or location, regardless of motivation and generally unrelated to other criminal activity.

- There is no specific demographic profile of an attacker.
- Those who pose a risk of violence do not always make direct threats prior to an attack, but they often communicate their intentions to those around them.
- Attackers often elicit concern from those around them because of their behaviors or communications.
- Bystander reporting and intervention can avert planned acts of targeted violence.

Preventing targeted workplace violence is everyone's responsibility. All employees, including supervisors, managers, front-line employees, and professionals in security, human resources (HR), and other positions and departments, have a role to play in violence prevention. For many employees, this includes **recognizing and reporting concerning behaviors they observe so action can be taken** to intervene before violence can occur. This publication is designed to promote organizational safety by offering information and guidance that can be used to establish a program to proactively prevent incidents of targeted workplace violence.

The publication is divided into two parts:

Part 1 - Mass Attacks at Workplaces: Key findings from NTAC's research examining mass attacks perpetrated in workplace settings, including the background characteristics and behavioral history of the attackers.

Part 2 - A Guide for Workplace Violence Prevention: A guide to implement an organizational behavioral threat assessment and management (BTAM) program based upon the proactive approach to violence prevention used by the U.S. Secret Service. In this guidance, we describe the principles of BTAM and offer a scalable 8-step framework to assist organizations of differing sizes and resources to take proactive action and reduce the risk of targeted workplace violence.

PART 1: MASS ATTACKS AT WORKPLACES

THIS STUDY'S POPULATION

The 50 incidents analyzed in this study are a subset from a population of 173 mass attacks described in NTAC's ***Mass Attacks in Public Spaces: 2016 – 2020*** (2023) report. These incidents resulted in harm to three or more people, not including the attacker(s), and were perpetrated in public or semi-public workplaces, including restaurants, bars, retail outlets, service centers, manufacturing and distribution facilities, healthcare settings, educational institutions, and military installations.

OVERVIEW

This section describes key findings of research using open sources examining 50 incidents of mass violence which occurred on the premises of a business or other work location. We present findings on the characteristics of the attacks and the backgrounds and behavioral histories of the attackers. In each incident, the attackers were known or knowable to the workplace prior to their attacks. An individual is ***known or knowable*** when their identity, affiliation, or patterns of behavior are either already recognized (i.e., known) or can reasonably be identified (i.e., knowable) based upon their frequent or substantive contact with the workplace.

Common types of individuals that are known or knowable to a workplace include:

- current or former employees;
- regular or notable customers, clients, patients, or visitors; and
- current or former romantic partners or relatives of individuals connected to the organization.

KNOWN OR KNOWABLE:

An individual is *known or knowable* when their identity, affiliation, or patterns of behavior are either already recognized (i.e., known) or can reasonably be identified (i.e., knowable) based upon their frequent or substantive contact with the workplace. Common types of individuals that are known or knowable to a workplace include current or former employees; regular or notable customers, clients, patients, or visitors; and the current or former romantic partners or relatives of individuals connected to the organization.

THE INCIDENTS

IMPACT

Across the 50 attacks examined, 128 people were injured and 119 were killed. Individuals harmed during attacks frequently included employees, customers, and visitors of the targeted site.

Many different types of workplaces were impacted by these incidents of mass violence, as illustrated in **Table 1**. Retail and service outlets were the most frequently impacted location type (*n* = 14, 28%), including grocery stores, hotels, salons, banks, law firms, and technology companies, among others. Other categories of workplaces that were commonly impacted included restaurants, bars, manufacturing and distribution centers, and healthcare settings.

Table 1: Locations Impacted

LOCATION TYPES	*n**	%
Retail/Services	14	28%
Restaurants/Bars	10	20%
Manufacturing/Distribution	10	20%
Healthcare	7	14%
Open Spaces	4	8%
Residential Community	2	4%
Non-profit Services	2	4%
Government	2	4%
Education	1	2%
Military	1	2%

*Total will exceed 50 as 3 attacks took place in more than one location type.

> *A 45-year-old gunman fatally shot four individuals in a shooting spree across three locations. The incident started when the attacker drove to his wife's workplace to demand she sign divorce papers. When she refused, the attacker retrieved a handgun from his car while his wife escaped. Moments later, the attacker returned and opened fire, killing two of the wife's coworkers. The attacker then drove to a law firm and fatally shot his wife's divorce attorney. Afterward, the attacker fled from police, drove to his apartment, positioned a rifle at his window, and fired at responding law enforcement, killing one officer. A three-hour long standoff ensued, and the attacker called dispatch multiple times, demanding reform in how assets are divided during divorce. The attacker was ultimately shot by law enforcement and later died of his injuries.*

WEAPONS USAGE

Firearms were used in most attacks (*n* = 43, 86%), as illustrated in **Table 2**. This included the use of handguns (*n* = 33) and long guns (*n* = 10). Over three-quarters of attacks (*n* = 38, 76%) involved the use of one weapon, and nearly one quarter of attacks (*n* = 12, 24%) involved the use of two weapons. Some attackers brought additional weapons that were unused during their attack.

Table 2: Weapons Used

WEAPON TYPE	*n**	%
Firearm	43	86%
Bladed Weapon	7	14%
Other	4	8%

*Total number exceeds 50 as 4 attackers used two types of weapons to inflict harm.

Sixteen attackers were actively employed by the location they targeted at the time of their attack, and most of these attackers (*n* = 13) initiated their attack during or immediately after a work shift. Of these attackers, four concealed their weapon(s) on their person prior to their attack, while five attackers kept their weapon in a vehicle on the work premises and later retrieved the weapon for use during the attack. Additionally, two attackers left the work premises during their shift to go home and retrieve weapons, then returned to the workplace to engage in their attack. One attacker was a U.S. military service member on watch duty and was armed with service weapons at the time of his attack.

All attacks using bladed weapons (*n* = 7) were perpetrated by customers, clients, patients, or visitors of the targeted location. Two attacks using bladed weapons were perpetrated at homeless shelters by residents. An additional two attacks using bladed weapons targeted staff and patients at mental health facilities, including one attack perpetrated by a patient who had been released one month earlier and another who had been denied entry into a treatment program hours earlier.

> *A 39-year-old man entered a mental health treatment center. Upon arrival, he began to yell, and insisted that he see the employee he saw on his last visit. When placed in a room with a female counselor, the man drew a knife concealed under his waistband and began to stab her repeatedly before exiting the room and slashing and stabbing numerous other employees. The attacker was ultimately chased and subdued by one of the center's clients until law enforcement arrived and arrested the attacker. Earlier that morning, the center had determined that the attacker was not appropriate for their treatment program due to his long history of violence and the severity of his mental health needs.*

Other attacks using bladed weapons targeted a property management office, the outdoor community space of an apartment complex, and a strip club. Other types of weapons were less common (*n* = 4), including a vehicle, propane tank, gasoline, and a homemade explosive device.

RESOLUTION

Table 3 illustrates how attacks were resolved. In over three-quarters of attacks (*n* = 38, 76%), attackers stopped causing harm on their own and then were arrested at or away from the scene of the attack (*n* = 15), or they died by suicide (*n* = 23). Less frequently, attackers were stopped by law enforcement intervention (*n* = 9) or bystanders intervened and stopped the attacker (*n* = 2). One attack ended after the attacker's weapon ran out of ammunition. Attackers died during or shortly after most attacks (*n* = 30, 60%), either dying by suicide or being killed by law enforcement. Of note, workplace attacks ended with the attacker's suicide at higher rates (46%) than in non-workplace related mass violence incidents (16%) examined in *Mass Attacks in Public Spaces: 2016 – 2020* (2023).

Table 3: Resolution

REASON THE ATTACK ENDED	*n*	%
Attackers stopped on their own, then...	**38**	**76%**
Arrested at/away from scene	15	30%
Died by suicide	23	46%
Law enforcement intervened, then...	**9**	**18%**
Arrested at/away from scene	2	4%
Killed by law enforcement	7	14%
Bystanders intervened, then...	**2**	**4%**
Arrested at/away from scene	1	2%
Other	1	2%
Weapon rendered inoperable, then...	**1**	**2%**
Arrested at/away from scene	1	2%

THE ATTACKERS

DEMOGRAPHICS

All but one of the 50 incidents examined were perpetrated by a single attacker. The one incident perpetrated by more than one attacker involved a pair of assailants that opened fire at a bar after one of the attackers had been thrown out of the establishment hours earlier. Nearly all attackers were male (*n* = 49, 96%), and ages ranged from 22 to 66 years old. The average age of workplace attackers was 41 years.

KEY FINDINGS FOR ATTACKERS

92% of attackers experienced ***stressors*** within five years of their attack.

78% of attackers had a history of behaviors that ***elicited concern*** from others.

65% of attackers had prior ***criminal charges***.

53% of attackers had at least one instance of ***domestic violence*** in their past.

STRESSORS

Nearly all attackers (*n* = 47, 92%) experienced noteworthy life ***stressors*** within five years of their attack. These stressors frequently included financial difficulties (*n* = 28, 55%), problems in their personal lives (*n* = 24, 47%), and employment-related issues (*n* = 23, 45%), including attackers experiencing conflicts with coworkers or facing disciplinary actions or termination at work. In many cases, attackers experienced multiple stressors at once. For instance, a U.S. military service member experienced a number of personal and professional stressors in the year leading up to his attack.

> *A 22-year-old service member in the U.S. military, armed with his service rifle and handgun, fatally shot two civilian workers and injured a third on base before fatally shooting himself. Within the year prior to the attack, the attacker experienced multiple stressors, including chronic pain resulting from a motorcycle accident, the ailing health of a loved one, harassment from peers, and numerous reprimands and citations at work due to poor performance and tardiness. At multiple points in time, the attacker sought medical attention for mental health problems, including visits for difficulty sleeping and concentrating, issues coping with stress, and feelings of alienation and lacking a sense of belonging among his peers.*

ELICITED CONCERN

Over three-quarters of attackers (*n* = 40, 78%) exhibited behaviors that ***elicited concern*** in others, and over half of attackers (*n* = 31, 61%) exhibited behaviors that caused observers to fear for the safety of the attacker, themselves, or others. For example, some attackers engaged in violence directed at romantic partners or relatives, prompting victims to seek protective orders or restraining orders against the attackers. Other behaviors that elicited concern included attackers making disturbing or threatening statements, exhibiting strange or unusual behaviors, and stalking and harassing others.

> *A 53-year-old man arrived at the elementary school where his estranged wife worked and told staff he was dropping off her lunch for the day. When he arrived at her classroom, the man drew a revolver and fired ten shots into the classroom, killing his wife and one of her students and injuring another student before dying by suicide. The attacker had a history of domestic violence spanning two decades, which included numerous assaults and threats to harm and kill women, including two previous wives, as well as threats to kill his own children. The attacker's violent and threatening behavior prompted multiple parties, including both of his ex-wives, an ex-girlfriend, and a local female pastor and her husband, to file restraining orders against him. The attacker was motivated to engage in the shooting after his estranged wife moved out of his home three months earlier and refused his attempts to force her return.*

CRIMINAL HISTORY

Nearly two-thirds of workplace attackers (*n* = 33, 65%) had a history of ***criminal charges***. Most of these attackers had charges for non-violent offenses (*n* = 29), and some had charges for violent offenses (*n* = 16), domestic violence (*n* = 9), or sex crimes (*n* = 4). However, not all criminal activity resulted in an arrest or a criminal charge. For example, over half of attackers (*n* = 27, 53%) had at least one instance of ***domestic violence*** in their past, but only around one-third of these attackers (*n* = 9) were arrested or charged for such an offense.

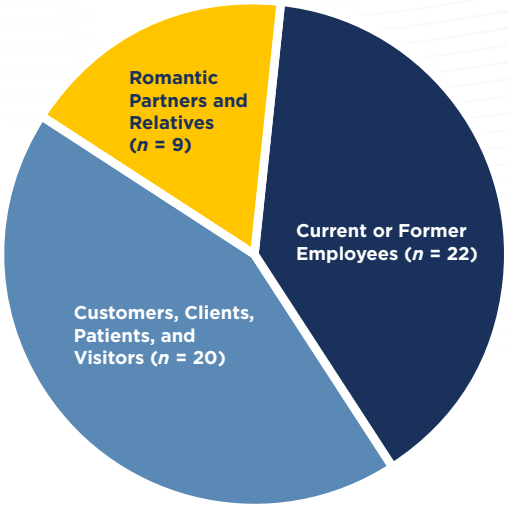
> *A 38-year-old gunman armed with a pistol and a rifle killed three and injured fourteen others in a shooting spree that began with him firing at other vehicles while driving and ended with him shooting coworkers at his place of employment. The attacker was ultimately shot and killed by responding law enforcement officers. Earlier that day, the attacker was served a civil protection order at his place of employment. The attacker had a long criminal history spanning two decades, including multiple felony convictions related to burglaries and gun charges, an arrest after the attacker got into a brawl with others, and many other charges that were ultimately dismissed. The attacker had numerous other encounters with law enforcement for domestic violence he perpetrated against his ex-girlfriend, prompting her to file for the protection order he was served on the day of his attack. Although the attacker could not legally own firearms due to his prior felony convictions, he threatened his ex-girlfriend until she provided him with the firearms he ultimately used in his attack.*

AFFILIATION TO TARGETED LOCATION

As illustrated in **Figure 1**, over two-fifths of attackers were current or former employees of the targeted location (*n* = 22, 43%); over one-third (*n* = 20, 39%) were customers, clients, patients, or visitors with frequent or substantive contact with the targeted location; and a smaller number (*n* = 9, 18%) were current or former romantic partners or relatives of individuals connected to the targeted site, such as employees or clients.

In the following sections, we describe key findings across these distinct categories of attackers.

FIGURE 1 Attacker Affiliation to Targeted Site



CURRENT OR FORMER EMPLOYEES

There were 22 attacks perpetrated by current or former employees of the targeted workplace, each perpetrated by a lone attacker. **For this section, percentages reflect the 22 attacks perpetrated by current and former employees of the targeted location.**

Demographics

All but one (*n* = 21, 95%) of the current or former employee attackers were male. Ages ranged from 22 to 64 years old, and the average age was 40 years.

Motive

Table 4 illustrates the motives of employee attackers, which were often multifaceted. All attackers but one (*n* = 21, 95%) were motivated, at least in part, by a ***grievance***. Three-quarters of attackers (*n* = 17, 77%) were specifically motivated, at least in part, by a workplace-related grievance. These grievances were related to workload, performance evaluations, disciplinary actions, termination decisions, and ongoing conflicts with supervisors or colleagues. The lone employee attacker who did not have a grievance as part of their motive appeared to be motivated solely by psychotic symptoms. Nearly one-third (*n* = 7, 32%) of employee attackers had multiple motives for their attack, frequently including combinations of workplace grievances with other motivations, such as psychotic symptoms or personal and domestic-related grievances. The attacker with the most motivations appeared to be motivated by psychotic symptoms, a workplace grievance, a desire to kill, and a desire for fame or notoriety.

> *A 24-year-old man armed with two shotguns opened fire almost two hours into a night shift at the grocery store where he worked, killing three coworkers before dying by suicide. In the months prior to his attack, the attacker created and shared videos glorifying school shootings, and described his admiration of past attackers and his plans for his attack in numerous journal entries. The attacker harbored delusional beliefs that when he died after his attack, he would become a cartoon female ghost character and join other violent cartoon characters in an afterlife.*

KEY FINDINGS FOR EMPLOYEES

95% of incidents were motivated by ***grievances***.

91% of attackers had at least one ***stressor*** within ***five*** years of their attack.

82% of attackers ***elicited concern*** from others, including 41% who elicited concern at work.

77% of attackers shared ***concerning communications***.

73% of attackers were ***currently employed*** at the facility they targeted.

Table 4: Component of Employees' Motives

EMPLOYEES' MOTIVES	*n*	%*
Grievance	**21**	**95%**
Workplace	17	77%
Personal	4	18%
Domestic	3	14%
Psychotic Symptoms	**5**	**23%**
Fame or Notoriety	**1**	**5%**
Desire to Kill	**1**	**5%**
Other	**1**	**5%**

*The percentages do not total to 100 as some attackers had multiple motives.

Background and Behavioral History

Most employee attackers (*n* = 20, 91%) had significant ***stressors*** within five years of their attack. The most common types of stressors included employment-related issues (*n* = 16, 73%) and financial difficulties (*n* = 13, 59%). Notably, over one-third of attackers (*n* = 8, 36%) were victims of bullying or harassment at work.

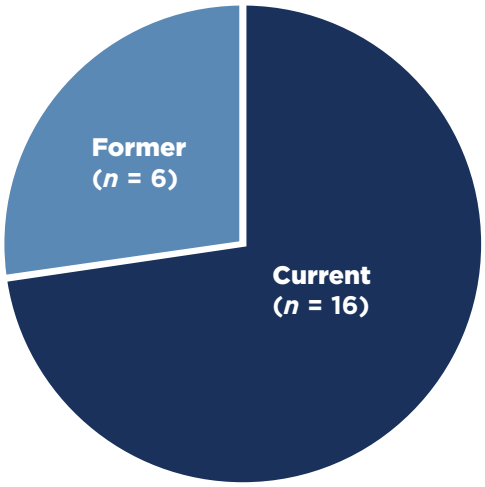
Most employee attackers (*n* = 18, 82%) ***elicited concern*** from others around them, half of whom (*n* = 9) elicited concern from colleagues in the workplace. Over three-quarters of employee attackers (*n* = 17, 77%) made ***concerning communications***. This included threatening statements (*n* = 9), and more commonly, statements that were not objectively threatening but elicited concern from those who heard them (*n* = 10). For example, one attacker accused his wife of collaborating with the government to spy on him, made her communicate with him in writing due to fears that others were listening to their conversations, and then would burn the pages they used to communicate. Another attacker threatened coworkers at the cemetery where he worked, prompting his termination. For seven years following his termination, the attacker complained to others about the cemetery and its employees before perpetrating his attack.

> *A 64-year-old man rode his bike to a cemetery where he used a handgun to shoot and kill one person and injure two more before surrendering to law enforcement. The attacker had vowed revenge and threatened to kill cemetery employees after he had been terminated from the cemetery seven years earlier. As an employee, the attacker had made threatening statements that concerned coworkers, prompting calls to law enforcement and his eventual termination. Two days prior to the attack, the attacker received an eviction notice from the apartment complex where he lived and worked. Prior to the attack at the cemetery, the attacker rigged his apartment, garage, and an adjacent residence with a series of incendiary devices, which were detected before they could detonate.*

Employment Status

As illustrated in **Figure 2**, most employee attackers were currently employed at the targeted site at the time of the attack (*n* = 16, 73%), ranging in tenure from 13 days to 22 years. Of these, most (*n* = 12) **initiated their attack either during or immediately following a work shift**. Six attackers were former employees, most (*n* = 5) of whom **had been terminated by the organization**. The length of time that elapsed between termination and attack varied, ranging from one attacker who immediately began his attack at the conclusion of a termination meeting, to another attacker who targeted a location where he had been terminated seven years earlier.

FIGURE 2 Employment Status



Two employees perpetrated attacks after submitting their resignation. The first attacker submitted his two weeks' notice at the beginning of his workday, completed his shift, and then inittiated his attack. The second attacker was a former employee who resigned in lieu of termination two years earlier after he had sexually harassed and threatened colleagues.

Work Performance

The **work performance** for employee attackers was mixed, as illustrated in **Table 5**. Of the 16 attackers currently employed at the targeted site, six were in good standing with their employers, characterized by supervisors or coworkers as highly skilled or hard workers. Eight attackers had substantive performance issues at work, resulting in disciplinary action for all but one. Though the nature of these problems varied, they included frequent or substantive work mistakes, safety violations, tardiness, and excessive or unexcused absences. Disciplinary actions ranged from complaints and letters of reprimand to termination. Information on performance was not found for eight employee attackers.

Table 5: Performance and Conduct

WORK PERFORMANCE	*n*	%*
Good standing	6	27%
Substantive issues	8	36%
Unknown	8	36%
BEHAVIORAL CONDUCT	***n***	**%***
Good standing	8	36%
Substantive issues	10	45%
Toxicity	7	32%
Unknown	4	18%

*The percentages do not total to 100 due to rounding.

> *A 45-year-old man armed with a semiautomatic rifle opened fire at a hospital where he had formerly been employed as a resident physician, killing one and injuring six. The attacker then set himself on fire and shot himself in the chest before ultimately succumbing to his wounds. Two years prior, he had resigned from the hospital in lieu of being fired due to allegations of sexually harassing and threatening his colleagues. The attacker blamed hospital staff, including a student in the residency program, for ruining his medical career, and threatened to return to the hospital and kill colleagues. At the time of his resignation, the hospital did not revoke his identification badge, which he used to access the hospital on the day of the attack. The attack date coincided with the hospital's residency program graduation.*

Behavioral Conduct

Behavioral conduct refers to actions taken by employees in the workplace, including how they interact with colleagues and others at work, and whether they adhere to an organization's policies or standards for behavior.[2] Over two-fifths (n = 10, 45%) of employee attackers had known substantive issues pertaining to their behavioral conduct at the workplace they attacked. For most of these attackers (n = 7), their misconduct could be characterized as **toxic**, showing persistent patterns of callous, reckless, paranoid, confrontational, aggressive, and/or threatening behaviors toward others. This included making racist, derogatory, or even threatening statements towards their colleagues. Two of these attackers exhibited toxic behavior in other organizations as well. Three attackers exhibited behaviors that were not considered toxic but still represented issues with conduct, including chronic absences or tardiness. Information on conduct could not be found for four employee attackers.

> *A 45-year-old gunman opened fire with a pistol at his former workplace, killing five of his former coworkers before dying by suicide. During his employment, the attacker had a reputation for being confrontational and frequently getting into fights with coworkers, including one instance in which he assaulted a coworker by punching and attempting to strangle him. The attacker had been fired two months earlier for stealing company equipment. Since his termination, he faced financial difficulties and struggled finding a new job. At one point, the attacker emailed a manager at the targeted site to request his old job back, but his request was denied. According to neighbors, the attacker's rent was due on the day of his attack.*

Disciplinary History and Terminations

Nearly half of employee attackers (*n* = 10, 45%) had at least one **infraction or disciplinary action** on record. This included complaints or reprimands about an employee's job performance, write-ups for behavioral misconduct or insubordination, and **terminations**. Five attackers were terminated from the targeted site prior to their attack, including one attacker who initiated his attack at the conclusion of a termination meeting.

> *A 45-year-old employee entered an office to attend a disciplinary meeting where he was informed that he would be fired. The employee had numerous rule violations on his record, including a safety violation from one day prior. During this meeting, the individual drew a concealed handgun and opened fire, killing four coworkers and injuring another. The attacker then proceeded to another area of the workplace campus and shot and killed a coworker who had reported his most recent safety violation. When police arrived, the attacker engaged in a shootout with them, injuring five officers before dying from gunshot wounds sustained during the exchange.*

Organizational Climate

Nearly half (*n* = 10, 45%) of the organizations impacted by these attacks had one or more identifiable issues pertaining to their **organizational climate**. For instance, one organization published a report one week after the attack that revealed the targeted facility had a below-average climate, poor morale, and employees who lacked a sense of belonging. Employees from another organization reported that personnel at the targeted facility suffered from racial discrimination and harassment for years leading up to the attack.

> *A 51-year-old man armed with two handguns shot and killed five colleagues at his workplace before fatally shooting himself. The organization where the attacker worked had a history of racial discrimination, bullying, and harassment of employees. In the years leading up to the attack, a noose and racist notes were left on the attacker's locker, and he was harassed and called racial epithets by coworkers. According to a coworker, the attacker reported at least one of these exchanges to the company's HR department, but the case was closed when the complaint could not be corroborated. After the attack, other employees reported that the work environment was racially segregated and that management ignored incidents of discrimination.*

As illustrated in **Table 6**, nine employee attackers (41%) made allegations to people at work or in their personal lives that they had experienced unfair treatment at the targeted workplace, including unfair promotion or demotion decisions or conflicts with supervisors and management. Most notably, over one-third of employee attackers (*n* = 8, 36%) reportedly experienced bullying or harassment by coworkers in the time leading up to the attack. In four cases, the attacker filed reports or voiced concerns about their experiences in the workplace, including grievances about workload and issues pertaining to bullying and harassment. For instance, one attacker was transferred to a different department after complaining about being harassed by a colleague. However, the harassment continued even after his transfer, prompting him to miss work, eventually leading to his termination from employment.

Table 6: Conflicts and Formal Reports

CONFLICTS AND FORMAL REPORTS	*n*	%*
Alleged mistreatment at work	9	41%
Experienced bullying or harassment at work	8	36%
Reported complaints or grievances	4	18%

*The percentages do not total to 100 as attackers may appear in more than one category.

> *A 53-year-old man opened fire with a semiautomatic handgun at a manufacturing facility, killing one and injuring three others before dying by suicide. The gunman had previously been terminated by the facility after missing three days of work. According to neighbors and police, the subject was an excellent employee who had never missed work prior to these absences, but he complained that he was being harassed by at least one coworker. Although the attacker had been transferred to a new department, the harassment continued, and he stopped showing up for work shifts and was terminated. The attacker may have experienced financial difficulties in the months following his termination as he tried to financially support his ill mother living abroad.*

CUSTOMERS, CLIENTS, PATIENTS, AND VISITORS

There were 19 attacks perpetrated by 20 individuals who were known or knowable to the targeted location as customers, clients, patients, and visitors. **For this section, percentages reflect those 20 customers, clients, patients, and visitors who perpetrated attacks.**

Demographics

All but one (*n* = 19, 95%) customer, client, patient, or visitor who perpetrated an attack were male. Ages ranged from 23 to 66 years old, and the average age was 41 years.

KEY FINDINGS FOR CUSTOMERS AND VISITORS

79% of incidents were motivated by ***grievances***.

65% engaged in ***concerning behaviors*** at the targeted location prior to their attack.

60% experienced a ***triggering event*** prior to their attack.

Motive

Over three-quarters (*n* = 15, 79%) of the 19 attacks perpetrated by customers, clients, patients, and visitors were motivated, in whole or in part, by a ***grievance*** that an attacker held against an organization or at least one of its employees. For example, one attacker opened fire at a venue hosting a video game tournament shortly after he lost a match, and another attacker targeted a healthcare facility that had expelled him from a treatment program. Other grievances included frustration due to being denied services, being expelled from a business, and other similar perceived slights.

> *A 36-year-old gunman armed with a rifle, a shotgun, and a bulletproof vest took five hostages at a residential treatment center where he had previously received treatment for post-traumatic stress disorder (PTSD). The gunman released two hostages, then locked himself in a room with the remaining three victims for eight hours and exchanged gunfire with a local police deputy. The three hostages were fatally shot by the attacker before he died by suicide. All three victims were employees at the treatment center and may have had a direct connection to the attacker's prior PTSD treatment, including one victim who had expelled him from the program two weeks earlier because the attacker had knives and threatened to kill staff.*

Background and Behavioral History

Nearly two-thirds (*n* = 13, 65%) of the attackers who were known or knowable as customers, clients, patients, and visitors engaged in ***concerning or threatening behaviors*** at the targeted location prior to their attack. These behaviors varied greatly, ranging from attackers who were ejected from the establishment due to erratic or rude behavior, to attackers who threatened to harm or kill employees or other customers. For example, an attacker who opened fire in a newsroom office had been harassing the staff of the newspaper for years leading up to his attack.

> *A 38-year-old man entered a newsroom and opened fire with a 12-gauge pump-action shotgun, killing five people. The attacker had a personal grievance with the newsroom after an unflattering article was written about him. The attacker had filed a defamation lawsuit against the paper six years earlier and had stalked and threatened employees of the paper, prompting them to contact law enforcement and develop personal safety plans. Prior to his attack, the attacker downloaded blueprints and recorded video of the newsroom building and its access points, read textbooks on mass shootings, studied police reaction times to previous attacks, and created and mailed a dossier with information about the intended victims and their families. In preparation for his incarceration after the attack, the attacker also sold his car and spent a significant portion of his income on the purchase of a lifetime membership for a chess organization.*

Over half (n = 12, 60%) of the customer, client, patient, and visitor attackers appeared to experience a specific ***triggering event*** prior to perpetrating an attack. These triggering events all occurred within one month of the attack, ranging from 2.5 hours to 2-4 weeks prior to the incident. The triggers included events such as a spouse saying they were filing for divorce, an attacker being served an eviction notice or protective order, an attacker learning that a lawsuit they filed was dismissed, and an attacker being fired from a job.

ROMANTIC PARTNERS AND RELATIVES

There were nine attacks perpetrated by attackers who were current or former romantic partners or relatives of individuals connected to the targeted site. Each of these attackers carried out their attack alone. **For this section, percentages reflect these nine attacks.**

KEY FINDINGS FOR PARTNERS AND RELATIVES

89% of incidents were motivated by ***grievances***.

78% of attackers had a history of ***domestic violence***.

Demographics

All nine attackers were male. Ages ranged from 27 to 58 years old, and the average age was 43 years.

Motive

All but one of these attacks (*n* = 8, 89%) were motivated, in whole or in part, by a ***grievance***, and most attacks (*n* = 7) involved grievances about a domestic matter involving a romantic partner. This includes six attackers who targeted their estranged or former romantic partners at their places of employment. Of these six attackers, two attackers also engaged in attacks at additional locations, including one attacker who targeted his romantic partner's father at his place of employment, and another attacker who targeted his wife's divorce attorney at the attorney's law office. One attacker motivated by a domestic grievance did not target a romantic partner's current place of employment, but instead targeted attorneys handling his divorce and mental health professionals who had conducted evaluations of the attacker's child during a custody dispute.

Background and Behavioral History

Notably, over three-quarters of these attackers (*n* = 7, 78%) had a history of making threatening statements toward romantic partners or family members, and they engaged in at least one act of ***domestic violence*** prior to their attack. However, only three of these attackers faced criminal charges for their acts of domestic violence.

> *A 43-year-old gunman, armed with a shotgun and a pistol, took two hostages in the woods outside of a healthcare center where his ex-girlfriend worked. After law enforcement responded to the scene, the gunman shot and killed a police chief as the chief exited his vehicle. The gunman then entered the healthcare facility and fatally shot his ex-girlfriend and her coworker before dying by suicide. The attacker had a lengthy history of violence and had abused at least one other woman in the past. In the months prior to the incident, he had assaulted and threatened to kill his ex-girlfriend multiple times, prompting her to obtain three protection orders against him, including one that was still in place at the time of the attack.*

Two attackers had familial relationships with one or more employees of their targeted location, including one attacker who was estranged from his family and targeted a restaurant owned by his nephews, and another attacker experiencing psychotic symptoms who engaged in a shooting at a bar owned by his cousin.

MENTAL HEALTH SYMPTOMS ACROSS ATTACKER TYPES

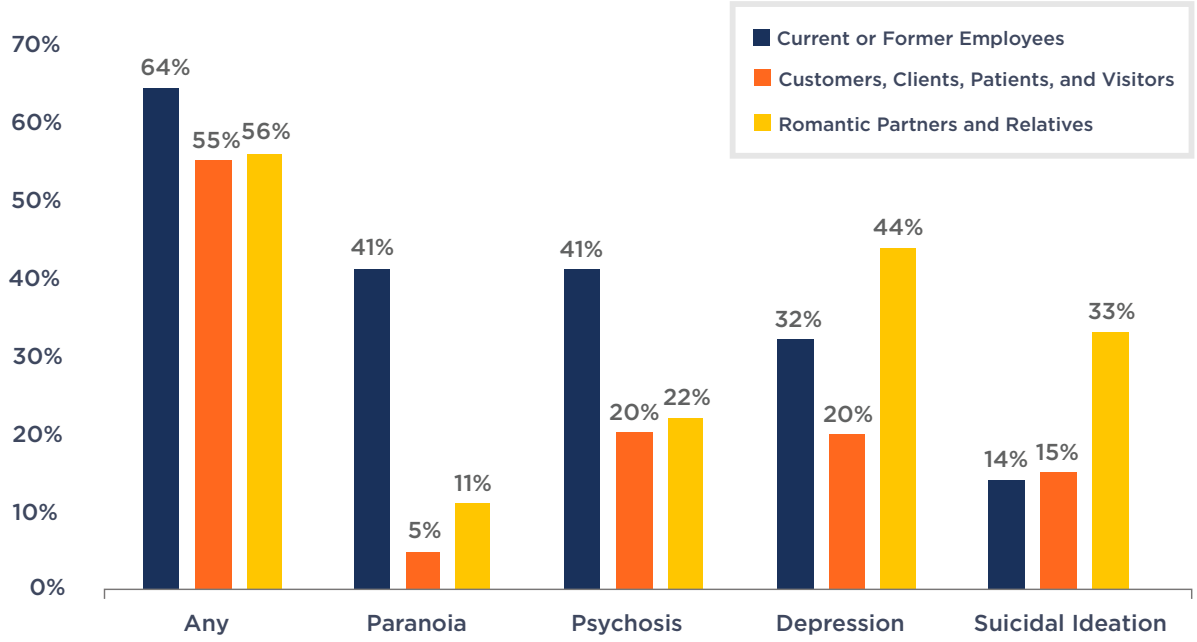
Over half of all workplace attackers (*n* = 30, 59%) were found to have experienced mental health symptoms prior to their attack, including psychosis (*n* = 15). Psychosis was evidenced by attackers experiencing delusions (*n* = 6), which are false, idiosyncratic beliefs that are firmly maintained despite evidence to the contrary, and hallucinations (*n* = 5), which are sensory perceptions that seem real but occur without any external stimulation. Paranoid delusions were the most common type of delusional beliefs experienced by attackers, while auditory hallucinations (e.g., hearing voices) were the most common form of hallucinations. Other symptoms that workplace attackers experienced included depression (*n* = 15), paranoia (*n* = 11), and suicidal ideations (*n* = 9). Nearly two-fifths of attackers (*n* = 20, 39%) received a prior diagnosis or treatment for a mental health issue before the attack.

> *A 30-year-old employee of a warehouse used a forklift to block an exit before shooting coworkers with a revolver, injuring three. The gunman then departed the scene and contacted police. On this call, the attacker told dispatchers that he had been hearing voices in his head since he was a teenager and that he had been previously treated for psychosis and schizophrenia. He also claimed that a manager at work was a powerful psychic who was attacking his mind, which he cited as a contributing factor to his motive. The attacker died by suicide later that evening.*

Of note, attackers who targeted a current or former place of employment experienced a higher proportion (*n* = 14, 64%) of mental health struggles than other attackers, as illustrated in **Figure 3**. Employee attackers experienced the most paranoia (*n* = 9, 41%) and psychosis (*n* = 9, 41%), including delusional beliefs (*n* = 5, 23%) and hallucinations (*n* = 4, 18%), compared to other categories of attackers. While attackers who targeted romantic partners or family members represented the smallest category, this group had higher rates of depression (*n* = 4, 44%) and suicidal ideation (*n* = 3, 33%) than others.

Although there was evidence of suicidal ideation for only three employee attackers, employee attacks often culminated in the attacker's death, either by suicide (55%) or by law enforcement response (23%).

FIGURE 3 Mental Health Symptoms



RESEARCH CONCLUSION

As these findings demonstrate, targeted workplace violence has been perpetrated by a variety of individuals who are known or knowable to a workplace, including current and former employees; customers, clients, patients, and visitors; and current or former romantic partners or relatives of individuals connected to the workplace. The findings also show that there is no specific demographic profile of the type of individuals who have carried out an attack targeting the workplace. However, among these populations, opportunities for intervention and prevention were often present, as many attackers elicited concern in others and often were motivated by grievances with the workplace. It is critical that all employees and other members of the workplace are trained to recognize and report concerning behaviors so appropriate action can be taken to proactively address concerns. In the remainder of this publication, we describe how organizations can successfully implement a behavioral threat assessment and management program to identify individuals of concern, gather information to assess for risk, and manage concerns to promote positive outcomes and reduce the risk of violence.

PART 2: A GUIDE FOR WORKPLACE VIOLENCE PREVENTION

A GUIDE FOR PREVENTION

The U.S. Secret Service recognizes that preventing targeted violence is possible if communities are equipped with the appropriate tools, training, and resources to recognize warning signs and intervene, namely through behavioral threat assessment and management.

Behavioral threat assessment and management (BTAM) is a behavior-based approach to proactively prevent incidents of targeted violence. The Secret Service originally pioneered this approach to prevent assassinations and safeguard the nation's leaders. As illustrated in **Figure 4**, the Secret Service model is designed to **identify** individuals displaying threatening or concerning behavior, gather information to **assess** if an individual poses a risk of violence, and then **manage** the risk by implementing appropriate interventions. The Secret Service model has since been adapted to prevent many forms of targeted violence impacting communities, including acts of targeted workplace violence.

FIGURE 4 The U.S. Secret Service Threat Assessment Model

The BTAM process is typically conducted by a multidisciplinary team comprised of personnel with diverse backgrounds, experience, and expertise, who take principal responsibility for identifying, assessing, and managing potential individuals of concern. In the context of preventing workplace violence, an ***individual of concern*** is any individual who has exhibited concerning behaviors that may indicate a potential risk of harm to themselves or others in the workplace setting. An individual eliciting concern can be: a current or former employee; a customer, client, patient, and visitor; or a current or former romantic partner or relative of an individual connected to the workplace.

INDIVIDUAL OF CONCERN:

Any individual who has exhibited concerning behaviors that may indicate a potential risk of harm to themselves or others in the workplace setting. An individual eliciting concern can be: a current or former employee; a customer, client, patient, and visitor; or a current or former romantic partner or relative of an individual connected to the workplace.

NTAC research and Secret Service operational experience have established that the BTAM process:

Is a systematic risk management approach. BTAM involves determining if an individual of concern poses a risk of violence while developing proactive management strategies to reduce the likelihood of a violent outcome.

Requires corroboration from diverse sources. In addition to gathering information directly through interviews with the individual of concern, the BTAM team should also evaluate information obtained from others who know the individual (e.g., colleagues, supervisors, family members), as well as lawfully accessible information contained in records, social media activity, and other forms of documentation.

Emphasizes rapport building. A BTAM team should employ rapport-building techniques to facilitate positive engagement and successful intervention.

Utilizes a low threshold of concern. Acting at the first sign of concerning behavior, instead of waiting for a direct or explicit threat, improves the chances of preventing violence.

Provides an avenue for early intervention. The BTAM process offers an opportunity to apply appropriate interventions before behavior escalates to criminality or violence.

Is not profiling. Rather than focusing on demographic characteristics (e.g., gender, age, race, ethnicity), the BTAM process prioritizes understanding an individual's thinking and behavior.

Is not prediction. Rather than attempting to predict who will act violently, the BTAM process should focus on identifying and addressing the concerning factors that appear to drive a person toward violence.

In the following sections, we offer a **scalable eight-step framework** for implementing a BTAM program in organizations of varying sizes and resources. This framework presents practical steps that workplace personnel can implement to successfully and proactively identify, assess, and manage individuals of concern, thereby reducing the risk of targeted workplace violence. The strategies identified in this publication are intended to assist organizations in preventing all forms of targeted workplace violence, including violence toward an organization's employees, executives, customers, visitors, and others.

This guidance was informed by several methods and data sources, including the protective operations used by the Secret Service and decades of NTAC research, training, and consultation in the areas of targeted violence prevention and behavioral threat assessment and management. To further bolster this guidance, NTAC also reviewed the extant literature on targeted violence and workplace violence prevention and conducted a series of informational interviews with personnel from a variety of organizations and industries, including retail, technology, food service, healthcare, education, entertainment, finance, government, and law enforcement. Interview subjects participated on the condition of confidentiality to allow for an open discussion. Participants represented a wide range of roles and disciplines, including professionals directly involved in organizational BTAM teams, as well as organizational executives, managers, supervisors, and personnel in human resources, security, insider threat, cybersecurity, and more. Some points shared by interview subjects are utilized as "Voices from the Field" throughout this publication.

The following foundational steps, described in greater detail throughout the remainder of this publication, provide **a practical roadmap for establishing a BTAM program** that organizations can adapt to their size, structure, and resources:

A FRAMEWORK FOR PREVENTION	
STEP 1	Commit to Employee Safety and Support
STEP 2	Establish BTAM Program Policy and Procedures
STEP 3	Assemble a Multidisciplinary BTAM Team
STEP 4	Identify and Process Reports of Concerning Behavior
STEP 5	Gather Information to Assess for Risk
STEP 6	Develop Risk Management Strategies
STEP 7	Promote a Safe and Supportive Organizational Climate
STEP 8	Provide Training for All Employees

STEP 1: COMMIT TO EMPLOYEE SAFETY AND SUPPORT

Adopting a prevention mindset through a commitment to employee safety and support is an important first step to reduce the risk of targeted violence in the workplace. This commitment can be demonstrated by securing leadership support for workplace safety efforts, providing resources and direction to employees, promoting collaboration and coordination of safety efforts between employees, and building partnerships with others outside of the organization's walls.

Targeted workplace violence can be prevented when organizations commit to a proactive approach to violence prevention. A BTAM program is a worthy investment for many organizations, offering critical **direct benefits**, such as the reduced risk of harm or loss of life, as well as **indirect benefits**, which can include improvements to employee morale and a more positive organizational climate and reputation.[3]

IMPACT OF INACTION

Workplace violence, which encompasses targeted workplace violence as well as other forms of physical violence, harassment, intimidation, or other threatening behavior, can be devastating to a workforce and the broader community. According to the Bureau of Labor Statistics, 928 workers tragically lost their lives in intentional homicides between 2023 and 2024.[4] During that same timeframe, an additional 77,780 workers in the private sector alone suffered nonfatal injuries from workplace violence that required days away from work, restricted job duties, or transfers.[5] The human cost is compounded by additional burdens on surviving victims and their employers, including financial costs associated with medical bills, loss of productivity, worker's compensation and disability claims, and subsequent litigation.[6] The human and financial costs underscore the importance for organizations to take action to reduce the risk of workplace violence.

SECURE LEADERSHIP BUY-IN

Support from senior leadership can be of paramount importance to the development of an effective BTAM program. Leaders who actively support violence prevention efforts are instrumental in ensuring that resources, funding, and staffing are allocated appropriately and that the work of the BTAM program is prioritized. Commitment from leaders may also ensure that all employees of the organization understand the importance of BTAM and collaborate during the BTAM process.

IN PRACTICE: IMPORTANCE OF LEADERSHIP BUY-IN

PRESENCE OF LEADERSHIP SUPPORT

ORGANIZATION 1: A security professional received little support for workplace violence prevention efforts. Undaunted by this initial lack of critical infrastructure, the security professional developed pitches for specific executives that quickly summarized the importance of a robust violence prevention program. One day, **during a chance encounter with a senior leader,** the security professional described an incident in the company's past when a terminated employee engaged in a spree of killings. Some of those impacted were employees of the organization whom the attacker felt had wronged him. After sharing this story, the security professional asked the executive how much the company had invested in workplace violence prevention. The executive conceded that the amount was not enough.

After this conversation, leadership provided the security professional with resources, funding, and the formal authority to establish the company's BTAM program. Partnering with personnel from security, HR, and the company's Employee Assistance Program (EAP), the security professional established an infrastructure to assess and manage concerns throughout the company.

LACK OF LEADERSHIP SUPPORT

ORGANIZATION 2: A threat manager experienced significant challenges getting support for workplace violence prevention from their organizational leadership. Despite the organization having thousands of employees, the threat manager was the sole person managing several important functions, including disaster recovery, cybersecurity, and active threats across numerous facilities within the United States. Recent structural changes, including a **corporate merger and the replacement of organizational leadership**, had resulted in additional challenges.

During a recent round of mass layoffs, **a violent incident was narrowly avoided** when an employee with significant personal stressors was laid off and threatened to return to the workplace with a gun. Due to their lack of training in handling threats, employees did not inform the threat manager about the employee's threat of violence or his termination. The employee was ultimately arrested for trespassing on the premises. The threat manager attempted to convince organizational leaders of the importance of proactive violence prevention efforts to avoid similar incidents. However, additional resources were not provided.

VOICES FROM THE FIELD

FROM AN EXECUTIVE OF A UNIVERSITY POLICE DEPARTMENT:

You can personalize violence prevention. You can make it close to home. In bigger organizations, someone knows someone who knows someone who has been impacted by a tragedy. You can create an energy about prevention that can inspire people and fuel their care. The enthusiasm is contagious.

OFFER RESOURCES AND GUIDANCE TO EMPLOYEES

Most larger organizations already have internal personnel who can help to prevent violence. These resources can include workplace managers, human resource (HR) professionals, or an ombudsman, all of whom can mediate conflict. Many organizations also offer Employee Assistance Programs (EAPs), which can provide counseling and support for employees experiencing distress.

One early step that organizations may take is to evaluate the internal resources that may be leveraged during the BTAM process. Once it is understood what resources are and are not available, organizations should take action to improve the quality or availability of these resources and ensure that necessary services and supports are available when needed. Completing a resource inventory (see **Figure 5**) can help organizations identify which needs the resources are designed to address, how often they are available and/or used, the quality of how well they address intended needs, whether there are any barriers or gaps in the services provided, and what actions can be taken to enhance services.

FIGURE 5 Sample Resource Inventory

This sample provides three examples of the types of resources that organizations may leverage during the BTAM process. Organizations should complete this type of inventory to assess all of their available resources.

Resource *What needs does it meet?*	Use *How frequently is it used?*	Quality *How well does it address our needs?*	Gaps or Barriers *Is anything limiting or impeding quality or availability?*	Action Plan *What actions can be taken to address gaps and build capacity?*
Ombudsman Provides alternative dispute resolution, mediation, and peer support.	**Low** Seldom used; highly available.	**Good** Employees who received services report they helped to resolve some disputes.	• Awareness is low. • Most concerns are solely brought to management.	• Promote awareness and education about this resource and process.
Employee Assistance Program (EAP) Provides counseling for difficulties with relationships, substances, and mostly personal matters.	**Moderate** Not used as frequently as expected; limited number of free sessions available.	**Excellent** Employees who used services report they helped tremendously.	• Some employees report concerns about confidentiality. • Perception of negative stigma (e.g., being treated differently or poorly due to treatment).	• Identify additional resources for counseling. • Enhance education regarding availability and confidentiality. • Promote policy addressing non-retaliation.
Third-Party Vendor for Employee Services Offers assistance to victims of domestic violence, including help with mental health, finances, moving, lodging, and more.	**High** Frequently used; contract allows a finite number of referrals.	**Excellent** Employees who have received services report they were highly beneficial.	• Only available via referral from BTAM team. • Limited number of referrals available. • Needs for services may increase due to growing workforce.	• Audit budget and costs to consider renewing and expanding contract with vendor. • Evaluate similar community resources that can supplement services.

PROMOTE INTERNAL COLLABORATION

All employees have a role in preventing violence at their workplace. Strong collaboration between employees across varying components within an organization can greatly benefit the BTAM process by safeguarding work environments. BTAM processes should incorporate the following strategies to foster collaboration:

Build relationships before services are needed. Navigating complex professional interactions in a new partnership during a critical time can be challenging. Establish partnerships before a time of need to support streamlined collaboration, information sharing, and crisis response.

Meet audiences where they are. Employees will benefit from an explanation of the BTAM process, how it can help, and their role in the process. When approaching employees, consider their unique perspectives and what information they need to know, focusing on the principles of safety, violence prevention, and employee support.

Clarify the capabilities of collaborators. Those involved in the BTAM process should have a clear understanding of everyone's role and how they can and cannot contribute. For example, HR personnel should know what employee information can and cannot be shared, when information can be shared, and with whom information can be shared. HR personnel should also understand the job functions and needs of collaborators on the BTAM team, including how they can assist collaborators, and how collaborators might aid them in their role in the BTAM process.

Lead with compassion, empathy, and care. Conversations about violence prevention can be uncomfortable and challenging, even for experienced practitioners in the field. Adopting language centered on supporting, helping, and caring for others can be effective in engaging colleagues, educating them on the principles of the BTAM process, and avoiding an excessive focus on punishment and reprimand.

Approach prospective partners with humility and the intent to help. The BTAM process will have the most success by reassuring employees that the goal of the process is to help, rather than to take over the work of other organizational components. This approach fosters trust with colleagues and lays the groundwork for long-lasting collaboration.

Establish goal alignment and clear roles. Different organizational components vary in their goals and functions. Clear communication can help all parties understand each other's mission and function, highlight points of goal alignment, and establish clear roles, responsibilities, and expectations.

VOICES FROM THE FIELD

FROM A BTAM TEAM LEADER AT A MAJOR RETAILER:

The most important thing is how you communicate with people … Early in my career, I used direct, academic language from the research. It confused people. I realized the importance lies in the concepts, not the lexicon. I started tailoring my language so that people without a background in this area can understand. When talking to a stakeholder, I might say, "I need you to know X, Y, and Z, and here's what I think you should do about a concerning individual."

BUILD COMMUNITY PARTNERSHIPS

Establishing partnerships with community agencies, such as local law enforcement, social services, or mental health professionals, is crucial to the success of organizational BTAM efforts. Community agencies can be highly effective resources in supplementing an organization's efforts to identify, assess, and manage concerning individuals. While these partnerships can be highly rewarding and beneficial, differences between agencies can sometimes pose challenges.

Some partnerships may experience challenges related to information sharing. For example, organizations may receive partial or limited information from a community partner, even when the partnering individual or agency wishes to be cooperative. At other times, community partners may appear to be nonresponsive or uncooperative. It is important to remember that each agency often has policies, rules, regulations, and laws they must follow, which may preclude them from freely sharing information.

Certain strategies may be effective in overcoming these barriers and fostering cooperation with outside agencies, such as:

Formalizing written partnership agreements. Clearly describing the activities and parameters of partnering agencies, including when, how, and what information is shared between the agency and the organization, can help resolve challenges and uncertainty during collaboration. Some organizations have established these formal agreements using a memorandum of understanding (MOU).

Establishing a designated point of contact for a partner agency. This strategy can limit confusion about who to contact when support is needed and may result in faster connections during a crisis.

Hosting or attending "seek to understand" meetings. Meeting with a community agency to listen and learn about their organizational goals, viewpoints, needs, challenges, or limitations can help foster understanding and build a more fruitful partnership.

VOICES FROM THE FIELD

FROM A BTAM TEAM IN A HEALTHCARE ENVIRONMENT:

Looking back now, I wish we would have started making relationships with team members and outside entities sooner. Talking with colleagues and community members in meetings, conferences, and sharing knowledge is vital for the practice of behavioral threat assessment everywhere. For us, going to meetings, consulting with others, sharing information, and having a common language has been incredibly helpful.

IN PRACTICE: BUILDING RELATIONSHIPS

A newly hired workplace safety manager at a major corporation recognized the value of partnerships with local law enforcement. He introduced himself to the local police department and made coffee and parking spaces available for officers and their patrol cars, which encouraged police to visit the organization's campus more frequently.

Over time, the organization established a strong relationship with law enforcement. The workplace safety manager convened a meeting with the officers, during which he described the organization's mission and needs and shared the building plans and a campus map with police. These resources ensure law enforcement will be able to safely and efficiently navigate the organization's campus if an incident occurs that requires law enforcement response.

STEP 2: ESTABLISH BTAM PROGRAM POLICY AND PROCEDURES

Developing sound programmatic infrastructure for a workplace BTAM program is important to creating an effective process for targeted violence prevention. This infrastructure should include two components: policy and standard operating procedures (SOPs). Organizational policy should establish the BTAM program, while the program's SOPs should outline the day-to-day operations and the roles and responsibilities for personnel involved in the BTAM process.

ESTABLISH POLICY

A policy establishing the organizational BTAM program should be formalized alongside or within any broader workplace violence policies that an organization already has in place. Having a dedicated policy for the BTAM program can help to create a more comprehensive prevention program capable of addressing a continuum of behaviors and concerns. Policy is important in establishing clear expectations and a foundation upon which the more granular details of the program can be built.

Some states have enacted legislation that requires certain employers to develop policies or plans to prevent workplace violence. While not explicitly required by these laws, workplace BTAM policies can build upon these legislative mandates and further promote workplace safety. For example, on September 30, 2023, California passed Senate Bill (S.B.) 553, which requires most California employers to create and maintain a written workplace violence prevention plan. The plan must be specific to the hazards and complexities of each work area, and employers are required to maintain a workplace violence incident log. This legislation also sets standards for documentation, record-keeping, and employee training, and it mandates the violence prevention plan be written and easily available to employees.[7] Since the passage of California's S.B. 553, many other states have actively worked to establish or expand their workplace violence legislative requirements.

A BTAM policy should establish and articulate each of the following:

Goals of the BTAM program. State the goal of BTAM in order to establish a clear vision and understanding of the program's intention. For example, describe the program's dedication to workplace safety and proactive prevention of violence.

Principles of BTAM. Articulate the key principles of the BTAM program. For example, state that the program encompasses work to proactively address any behavior that indicates a potential risk to safety and is not limited to explicit or direct threats.

Authority and staffing of the BTAM team. It is best practice that many of the essential functions of the BTAM program be carried out by a multidisciplinary BTAM team. Specify which departments, roles, and job functions are required to serve as core BTAM team members, and which might support the team in an ad hoc capacity (see Step 3). Establish the authority of a BTAM team to perform the necessary functions to allow them to identify, assess, and manage individuals of concern before violence can occur (see Steps 4, 5, and 6).

Program scope. Articulate who will be subject to a behavioral threat assessment and what actions may be taken during the BTAM process. This may include current and former employees; frequent or notable customers, clients, patients, and visitors; or current or former romantic partners or relatives of individuals connected to the workplace.

Program placement and integration. Establish which organizational department, component, or division (e.g., security, HR) will house the BTAM program and how the BTAM program will be integrated into the organization. The structure of the BTAM team (see **Figure 6**) should be based upon organizational needs.

FIGURE 6 Potential BTAM Team Structures

TEAM STRUCTURE	WHAT IT LOOKS LIKE	EXAMPLE USAGE
CENTRAL TEAM	One BTAM team assesses and manages all incoming reports in an organization.	An organization with a modest volume of incoming reports has one BTAM team stationed in the organization's headquarters.
LOCAL TEAMS	Multiple decentralized teams each assess and manage incoming reports from local facilities.	An organization has local BTAM teams across several geographic regions to respond to reports at numerous facilities in their area of responsibility.
REGIONAL TEAMS WITH SUPPORT	Multiple regional teams assess and manage incoming reports while a centralized team consults and supports with difficult cases.	A large organization with a high volume of reports uses regional teams, each serving several facilities in their region, with coordination and assistance available from a centralized BTAM team at the organization's headquarters.

Receiving reports of concerning behaviors. Briefly describe concerning behaviors that should be reported to the BTAM program and how individuals, especially employees, can report their concerns.

Threshold for initiating a BTAM inquiry and response. Establish parameters for when the BTAM team will convene and respond to a report. The policy should allow for a low threshold of concern (see Step 4).

Threshold for law enforcement intervention. Establish what behaviors and reports should necessitate notification to law enforcement for assistance with a safety concern or a criminal matter.

Explanation of privacy protections. Describe what safeguards are offered to protect individuals who share information during the BTAM process.

Information sharing. Establish provisions for sharing information internally (i.e., between personnel, departments, and divisions) and externally (i.e., with outside partners). When applicable, public safety exceptions that either facilitate or require information sharing should be described.

SAMPLE POLICY STATEMENT

[Organization Name] is dedicated to establishing and maintaining a safe workplace for all employees. In support of that commitment, this policy establishes **[name of the BTAM program]**, which is dedicated to the proactive prevention of targeted violence in the workplace. **[Name of the BTAM program]** will utilize a multidisciplinary team composed of **[describe relevant personnel, departments, or units]**. Established **[within/under]** the **[department or division with oversight over the BTAM team]**, the mission of the **[name of the BTAM team]** is to identify, assess, and manage individuals who may pose a risk of harm to themselves or others in the workplace, either currently or in the future. To achieve this mission, the **[name of the BTAM team]** will receive, investigate, and assess reports of concerns within the workplace, and provide direction, management, support, and follow-up to address concerns before the risk of potential violence escalates to physical harm.

DEVELOP STANDARD OPERATING PROCEDURES (SOPs)

Developing standard operating procedures (SOPs) can support a thorough, consistent, and standardized BTAM process, and allows for program continuity over time and through changes to team membership. Memorializing detailed SOPs can also allow for all BTAM team members to have a shared understanding of what is expected of them and what they can expect from others on the team. Moreover, documenting procedures allows an organization to assess programmatic and procedural strengths and to identify areas for continued improvement.

SOPs should:

- account for each phase of the BTAM process and what should be accomplished within each phase, including how concerning behaviors will be identified and reported, how the BTAM team will conduct an inquiry or a full assessment (see Step 5), and what resources are available to intervene and manage concerning situations;

- identify what actionable steps and tasks must be taken to move through the process, who is responsible for completing them, timeframes for completion, and documentation requirements;
- establish frequency of team meetings and who leads them (see sample below);
- establish program improvement cycle requirements and identify data points that will be used to determine program fidelity, effectiveness, and impact; and
- include a high-level process map and decision tree illustrating the overall process of the organization's BTAM approach (see Step 5).

SAMPLE LANGUAGE ABOUT TEAM MEETINGS

The Behavioral Threat Assessment and Management (BTAM) Team will convene twice per month to review and assess potential concerns. Required attendees will include the team lead, and at least one security manager, human resources representative, legal advisor, and mental health professional. During each meeting, the team will discuss recent reports of concerning behaviors, ongoing case updates, risk management strategies, and recommendations for intervention or support. Actions taken may include assigning follow-up tasks, coordinating with external agencies, and updating case management plans. All meeting proceedings, including attendance, topics discussed, decisions made, and assigned actions, will be documented in a secure, access-controlled record for accountability and future reference.

CONTINUOUS IMPROVEMENT

Organizations that already have established workplace violence prevention policies and procedures should consider conducting a gap analysis to:

- ensure alignment between existing policies;
- identify sources of conflict that may need to be addressed to support clear and efficient functioning;
- review resources to identify opportunities to build capacity; and
- evaluate current processes, from initial report through case closure, to determine if changes are needed.

It is also important to evaluate organizational awareness of the program, employee understanding of the role they play in prevention through reporting, and to provide training opportunities to enhance staff awareness.

STEP 3: ASSEMBLE A MULTIDISCIPLINARY BTAM TEAM

BTAM in the workplace requires a multidisciplinary team to process reports of concerning behaviors, gather information to assess for risk of harm or other unwanted behavior, and implement appropriate interventions to reduce risk. When developing the BTAM program, organizations should invest time in determining the appropriate team composition, establish expectations regarding training for BTAM team members, and set standards for BTAM team meetings.

The responsibility for violence prevention belongs to everyone in a workplace. However, it is best practice to identify personnel who can be routinely dedicated to the important tasks associated with the BTAM process. Establishing a multidisciplinary BTAM team can allow team members with varied organizational roles and responsibilities to leverage their unique expertise, perspectives, and skills to prevent violence.

VOICES FROM THE FIELD

FROM A BTAM TEAM AT A MAJOR HEALTHCARE ORGANIZATION:

It's important to get the right people. Previously, team members were identified because they were told to join. Once the executives knew and understood the vision of the program and saw the good work the team was doing, a new hiring process was developed to select people really interested in joining the threat assessment team. We developed onboarding processes to get them up to speed and teach them what the process entails. That has been very helpful.

DETERMINE BTAM TEAM COMPOSITION

The BTAM team serves as the primary decision-maker throughout the BTAM process. BTAM teams should include a core group of dedicated, trained professionals. When deciding the composition of the **core team**, leaders should determine if individuals will be assigned to a BTAM team in a full-time capacity, or whether team assignment will be a collateral or part-time duty. Workplace BTAM teams often include personnel from the following organizational roles:

Management. A senior-level manager can serve in the role of facilitator, leader, and/or final decision-maker. Management can also ensure information is shared between managers and across departments, as appropriate.

Human Resources (HR). HR professionals can access employee personnel records, offer insight on employee performance and conduct, utilize safe hiring and firing practices, share knowledge about organizational policies and procedures, and assist with employee morale and office culture.

Security. Security personnel can provide support in communicating with local law enforcement, gathering information, supporting physical security responses, and developing and supporting safety plans.

Information Technology (IT). IT professionals can access relevant digital records, system access logs, and electronic and telephonic communication records. IT professionals can also limit an individual's access to systems and facilities.

Cybersecurity and Insider Threat. Cybersecurity and insider threat personnel can monitor the inappropriate use of employer-issued electronic devices throughout the BTAM process.

Legal. Legal personnel can provide guidance and advice to the BTAM team to ensure compliance with federal, state, and local laws that apply to the organization, including privacy, employee rights, and how to properly handle and store documents.

Employee Assistance Program (EAP). EAP personnel can provide insight into available resources to leverage when developing a plan to manage the risk posed by individuals of concern.

In a core BTAM team, the BTAM team leader is responsible for ensuring compliance with policies and procedures, facilitating team meetings, and helping team members reach consensus. Importantly, the BTAM team leader is also responsible for communicating information between the BTAM team and organizational leadership when necessary.

The composition of the BTAM team will differ across organizations, as it is tailored to meet the organization's unique characteristics and needs. While some of the roles described above may have one or more representatives that serve as permanent members of the BTAM team, other roles may support the BTAM process in an ad hoc capacity. **Ad hoc participants** do not regularly attend BTAM team meetings, but when appropriate, can coordinate with the BTAM team, share and receive important information, and provide ancillary support throughout the BTAM process.

VOICES FROM THE FIELD

FROM A HUMAN RESOURCES PROFESSIONAL:

Put someone from HR on the behavioral threat assessment team! HR are among the first to see concerns or threats in the workplace. While they are often cautious about sharing information across departments, they also have an obligation to protect the organization, which is the goal of a behavioral threat assessment. Inviting HR on the team can be more helpful than just asking them for information.

FROM A CYBERSECURITY PROFESSIONAL:

Cyber is typically the last group that is contacted during a behavioral threat assessment, but we're trying to get involved in the process earlier. A lot of cybersecurity work lends itself well to a prevention-based approach. I'd like to see more of a bridging of the gap between cybersecurity and threat assessment.

Ad hoc participants can vary by case and across organizations and can include any of the roles described earlier. They can also include organizational departments and community partners, such as:

State and local law enforcement. Law enforcement can assist with information gathering, responding to safety concerns, and supporting management strategies.

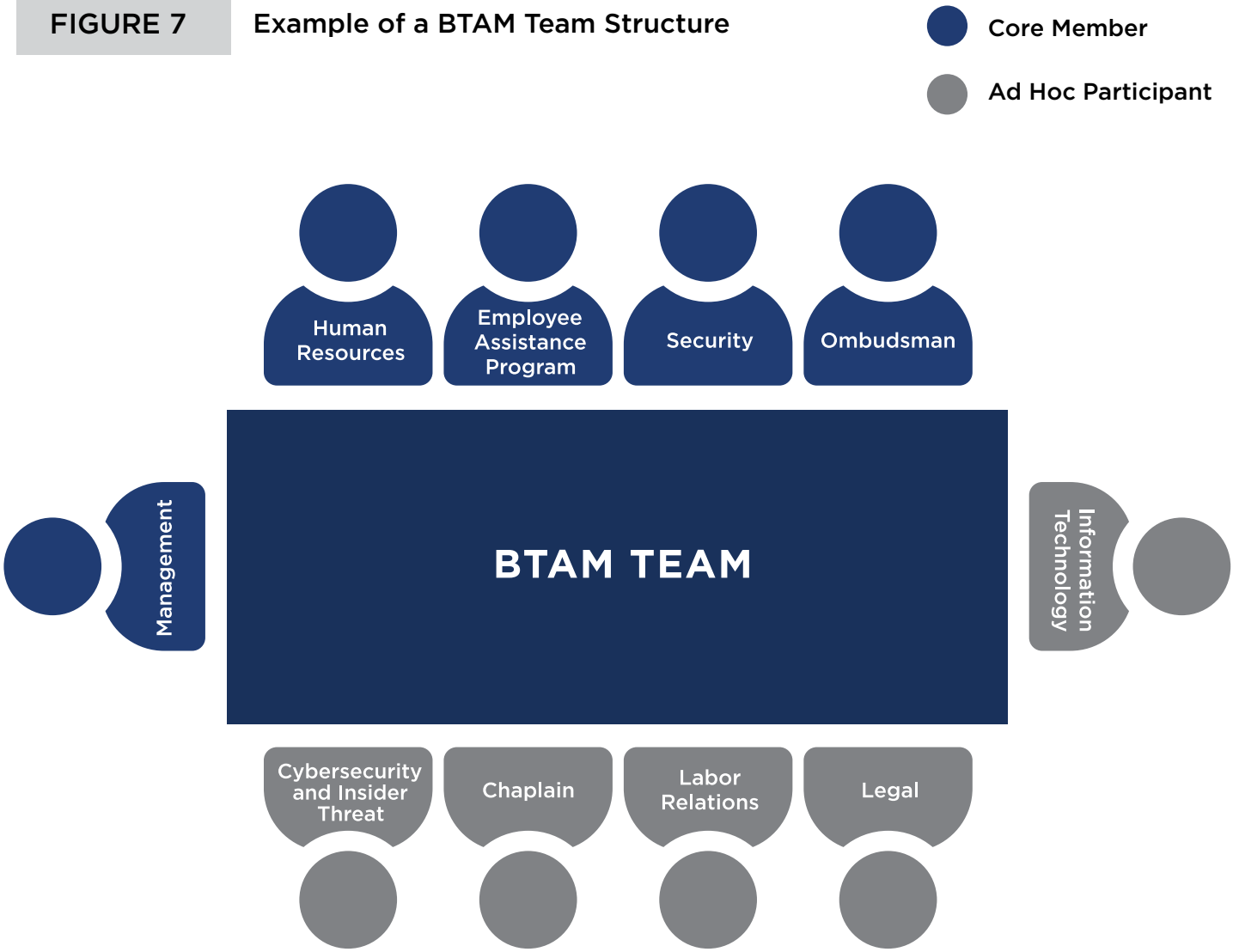
Community mental health. Mental health professionals can provide insight into how mental health may impact a case and can share knowledge regarding available resources.

Labor relations. Representatives from labor relations can provide insight into employee grievances, conflicts, and disputes. They also offer guidance on contracts between unionized employees and the organization, and support employee due process.

Alternative dispute resolution. Personnel who specialize in alternative dispute resolution, including an ombudsman or mediator, can help during negotiations between employees, address conflicts and grievances, and offer insight and perspectives about employee behavior.

Importantly, employees need not be core members of a BTAM team to be relevant to the BTAM process. While core BTAM team members carry out the essential and routine functions of the BTAM program, ad hoc participants and other personnel within the organization can be critically important when identifying, assessing, and managing individuals of concern. **Figure 7** illustrates just one example of how an organization may staff a BTAM team and facilitate coordination across personnel and departments. In this example, a manager, a security official, an HR professional, and personnel from the legal department and EAP have representatives that serve directly on the organization's BTAM team. While the BTAM team in this example does not have permanent representatives from IT, cybersecurity and insider threat, or the offices of the chaplain, ombudsman, or labor relations, the team should engage with these personnel as needed to facilitate information sharing, particularly during the assessment and management processes. While the BTAM team structure and the relevant organizational departments may vary across organizations, these structures can be adapted to meet the unique characteristics and needs of an organization.

FIGURE 7 Example of a BTAM Team Structure



TRAIN BTAM TEAM MEMBERS

Training is essential for ensuring that team members build and maintain their knowledge and skills with BTAM practices. Team members should receive recurring training on the organization's BTAM process to ensure members understand their roles and responsibilities. They should also engage in comprehensive skill-building to promote program fidelity and build expertise for effective assessment and management.

Training content for team members should address the following:

Overview of the BTAM process. This should include information about the BTAM process, including roles and responsibilities, how the team operates, and the importance of information sharing throughout the organization.

Reporting mechanisms. BTAM team members should be well-trained in what and how behaviors of concern should be reported in their organization, how reporting mechanisms are promoted, and how to respond to reports that are received.

Risk management. BTAM team members should be knowledgeable about the risk management resources available, both within the organization and the broader community.

Contacting law enforcement. Training for BTAM members should describe when it is appropriate to contact law enforcement, as well as procedures that personnel should follow once law enforcement has been contacted.

BTAM policies and procedures. This should include an overview of the policies and procedures that guide the BTAM team's day-to-day operations, as well as a discussion of the ancillary policies and procedures that may intersect with the BTAM process (e.g., disciplinary procedures, emergency response plan).

Documentation and records management. BTAM team members should be aware of their requirements to maintain documentation and should become familiar with instructions and forms relevant to the BTAM process. This should include when forms are recommended as opposed to when they are required, who must complete the forms, and how the forms should be completed, shared, and/or stored.

Legal and privacy considerations. BTAM team members should also be aware of municipal, state, and federal laws, rules, and regulations that apply to their work.

Additional training. Other training can be valuable to BTAM team members, including training on mental health, de-escalation techniques, motivational interviewing, conflict resolution and mediation, trauma-informed care, crisis intervention and management, suicide prevention, intimate partner violence prevention, stalking awareness and prevention, and scenario-based tabletop exercises.

NATIONAL THREAT ASSESSMENT CENTER (NTAC) VIRTUAL TRAINING CALENDAR

The U.S. Secret Service NTAC offers free recurring virtual trainings delivered by NTAC personnel. During these presentations, NTAC staff share findings from decades of research on targeted violence and guidance on how the BTAM process can be used to prevent future tragedies in our communities. To learn more or to register for one or more of these training events, visit: **https://www.secretservice.gov/ntac/virtual**.

ESTABLISH REGULAR BTAM TEAM MEETINGS

BTAM team meetings should be intentional and structured. The BTAM team should meet whenever a concerning individual has been identified to conduct the assessment, to share information learned, and to develop an individualized case management plan if necessary. The BTAM team should also hold scheduled meetings on a regular basis to build cohesion, receive training, conduct case reviews, and refine existing policies and procedures. During these regular meetings, BTAM team members may share details of a particular case, discuss specific challenges or successes encountered, or offer information about pertinent resources or organizational changes that impact their work. These meetings provide an opportunity to engage in discussions, conduct tabletop or role-playing scenarios, and ensure that all members are prepared to implement the best practices related to BTAM.

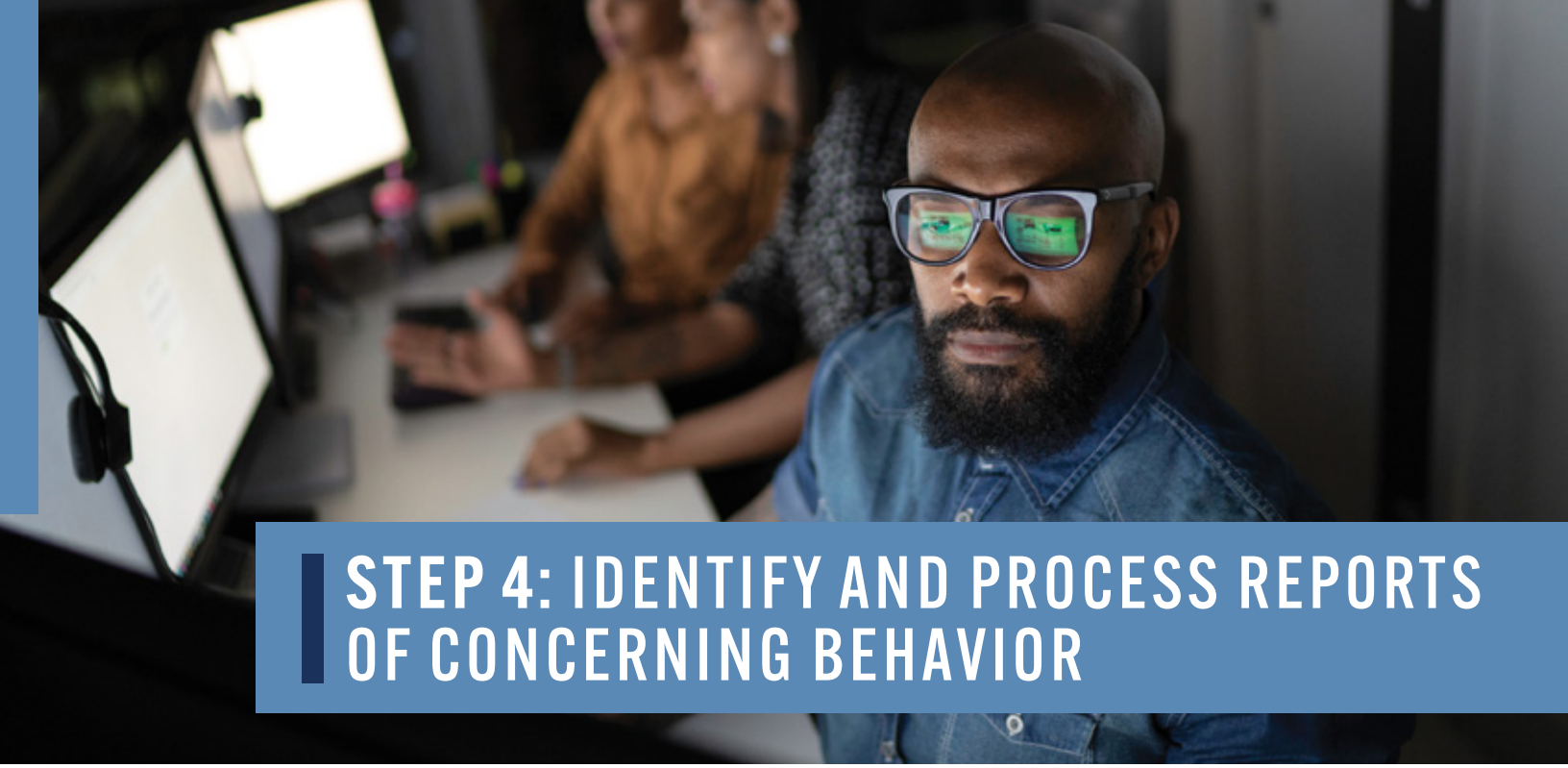
VOICES FROM THE FIELD

FROM A SECURITY TEAM AT A GLOBAL TECHNOLOGY COMPANY:

The Chief Compliance Officer holds quarterly meetings in every region where we discuss what people are seeing, promote a "see something, say something" culture, and talk about active cases. We rely on our personnel globally to report concerning information. Having these 30-minute meetings really benefits information sharing and showing people that we are a team. Information sharing is what keeps the company safe.

FROM A BTAM PROFESSIONAL AT A MAJOR SERVICE CHAIN:

Our team is unique, and we're highly collaborative. So if an individual team member runs into an issue where we feel like we don't really know which route to take, especially as far as mitigating risk, then we reach out to one another. We meet regularly as a team to brainstorm and collaborate.



STEP 4: IDENTIFY AND PROCESS REPORTS OF CONCERNING BEHAVIOR

One of the most important actions an employee can take to prevent violence is to report any concerning behaviors they witness. Organizations should ensure that all employees are trained to recognize concerning behavior and have avenues through which they can report their safety concerns. Once a report is received, BTAM teams should process and triage these reports of concern. Identifying and processing reports of concern is the first step during a behavioral threat assessment.

RECOGNIZE BEHAVIORS OF CONCERN

Organizations must train their workforce to recognize and report their concerns when an individual or situation elicits concern for the safety of themselves or others. All employees must understand that threatening statements should be reported, **but a person may pose a risk of violence without making an explicit threat**. In fact, ***concerning behaviors*** occur along a continuum from contextually concerning to objectively concerning (see **Figure 8**), and include non-criminal and criminal activities. Concerning behaviors may include escalating interpersonal disputes, grievances, concerning social media content, stalking and harassment, obsessions with violence, idolizing past attackers, fixating on people or locations, suicidal ideations, self-harm, unusual levels of aggression, threats, weapons violations, and physical assaults.

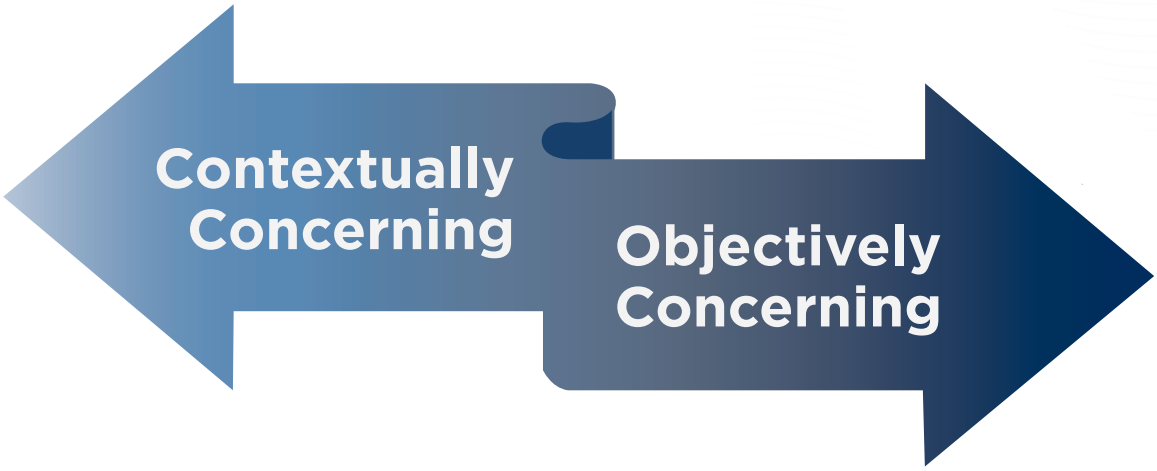
CONCERNING BEHAVIOR:

Actions or communications by an individual that are objectively or contextually troubling or inappropriate and indicate a potential risk of violence.

Some behaviors are objectively concerning (e.g., unauthorized weapons, threats, assaults) and should warrant immediate action, oftentimes including local law enforcement intervention. Other behaviors are contextually concerning, in that they may not prompt immediate safety concerns but should be assessed in the full context of the individual's situation and their environment (e.g., rapidly deteriorating performance, angry outbursts) to appropriately assess risk.

A good guiding principle is that employees should be encouraged to report any observed behavior that prompts them to feel uncomfortable or concerned for their own safety or the safety of others. Employees should also be provided with specific examples of the types of behavior that may prompt these concerns.

FIGURE 8 Examples of Concerning Behaviors



Contextually Concerning	Objectively Concerning
Changes in behavior, including decreased productivity, increased absenteeism, decreased attention to personal hygiene and appearance, or withdrawal from social circles	Bullying or harassing others
Fixations on perceived grievances	Preoccupation with violent themes, such as terroristic acts or mass shootings
Challenges with mental health, such as depressed mood, paranoia, or anxiety	Intimidating, belligerent, or other aggressive behavior
Intense or abnormal emotional outbursts	Expressions of homicidal or suicidal thoughts
Questionable activity on work-issued devices, such as attempting to access prohibited sites or searching for inappropriate content	Direct or veiled threats
Pattern of strained or conflicted relationships with colleagues	Physical violence toward people, animals, or property
	Sexual assault or harassment
	Bringing or brandishing a weapon in the workplace

INTIMATE PARTNER VIOLENCE AND THE WORKPLACE

Intimate partner violence (IPV) is abuse or aggression that occurs in the context of a romantic relationship and can include both current and former spouses and dating partners. IPV can include physical violence, psychological aggression, sexual violence, stalking, and other behaviors. The frequency and severity of IPV varies, ranging from a single episode of violence to chronic and severe instances of violence spanning multiple years.[8]

What is the impact of IPV on the workplace?
While IPV often starts in the privacy of a residence, it can spill out into public spaces. In *Mass Attacks in Public Spaces: 2016 – 2020* (2023), NTAC found that 41% of individuals who engaged in mass attacks in public or semi-public spaces, including workplaces, had a prior history of domestic violence, including intimate partner violence. In 29% of the incidents, mass attackers were motivated to carry out their attack, at least in part, by a domestic grievance. According to the Centers for Disease Control and Prevention (CDC):

- victims of IPV lose nearly 8 million days of paid work each year in the United States; and
- the estimated total cost of IPV—including medical care, mental health services, and lost productivity—exceeds $8.3 billion per year.[9]

What are potential indicators that an employee might be experiencing IPV?
Organizations should be aware of certain warning signs that could indicate an employee is experiencing IPV, including:

- decrease in work performance;
- uncharacteristic absenteeism or lateness;
- changes in appearance that could conceal injuries (e.g., wearing clothes that do not fit the season, changes in the use of makeup);
- increased reluctance to socialize with coworkers;
- abrupt change in address or living situation;
- sudden requests to move away from open and public areas in the workplace; and
- disruptive visits, phone calls, or messages from their current or former partner.[10,11]

How can organizations help?
Organizations must take immediate action if an employee is believed to be experiencing violence in a relationship. Below are some examples of how organizations can help employees in these difficult situations:

- Provide victims with parking spaces near the door of the workplace building
- Offer internal and third-party services, including counseling and mental health care
- Allocate funds for financial support to victims
- Grant flexibility to victims for using sick days and personal leave
- Coordinate with local shelters to identify available openings for victims
- Offer relocation services to help victims move to a new residence
- Use anonymized work schedules to decrease risk of abusers locating victims
- Increase physical security presence in impacted locations

VOICES FROM THE FIELD

FROM A THERAPIST WHO SPECIALIZES IN SUPPORTING VICTIMS OF IPV...

...ON RISK FACTORS:

IPV is one of the leading causes for workplace violence. It's always a huge risk factor ... IPV cases tend to be more severe when IPV bleeds over into the workplace. Stalking and monitoring behaviors tend to be the most common red flags when someone is reporting IPV at work.

...ON ENCOURAGING VICTIMS TO REPORT ABUSE:

Coming forward requires power and confidence. It's important to give victims a lot of voice and choice. You give them the information, then let them make their own choices. That's giving them the power that their abuser is taking from them ... When they do come forward, we follow the victim's lead with safety in mind. We make a safety plan with them to achieve their goals.

...ON SUCCESSFUL STRATEGIES FOR MANAGING IPV:

The most successful strategy is trauma-informed care ... We try to hear the person out and understand their situation using a nonjudgmental, recovery-oriented stance. It gives them the space to talk about these things and allows for honesty ... In an abusive relationship, victims have little control. It's disempowering by design. In our encounters, in very small ways, we must do the opposite, and provide feedback on what they're doing well ... For safety planning, we ask them what they've done already and what has worked, and what hasn't. Usually, they've tried a plethora of things already, and you'd be wasting your time by making assumptions and listing off tips.

NATIONAL DOMESTIC VIOLENCE HOTLINE

If you or someone you know is experiencing domestic violence, help is available via the National Domestic Violence Hotline.

1-800-799-SAFE (7233) | Text "**START**" to **88788**

VOICES FROM THE FIELD

FROM A BTAM TEAM LEADER AT A GLOBAL CORPORATION:

A lot of what we tend to see are cases involving suicidal ideation, someone going through an individualized crisis, or someone having difficulties managing work and lashing out. We also see issues with domestic violence and intimate partner violence in all of our regions across the globe.

It is essential for organizations to maintain a **low threshold of concern** for initiating a behavioral threat assessment and not limit their focus solely to explicit threats of violence. Utilizing a low threshold of concern allows BTAM teams to identify individuals eliciting safety concerns before their behavior escalates to the point where there is an imminent risk of harm.

LOW THRESHOLD OF CONCERN

Consider this scenario: An employee has recently demonstrated performance problems at work. Although he was previously an above-average employee, he has begun to miss deadlines, and the quality of his work has declined. The employee's work acquaintances report he has been "distant" and "moody" lately and might be having problems at home. In a recent meeting, the employee's supervisor asked the employee what was happening. The employee remarked that he did not know what the supervisor meant by the question and denied seeing any problems with his recent performance. In the weeks since that meeting with his supervisor, the employee has begun to call in sick to work with increasing frequency, and when he does show up for work, his appearance has become increasingly unkempt. The supervisor is worried about the wellness and safety of the employee.

While the situation described in the hypothetical scenario above may not prompt immediate concerns for violence, the behaviors demonstrated by this employee may illustrate individual or environmental factors that, if unaddressed, could contribute to an increased possibility of harm to self or others. It is best practice to use a low threshold of concern during the BTAM process, not to label an individual as a potential threat, but to allow for early intervention. Early intervention enables organizations to identify, assess, and manage the possibility of a negative outcome long before violence becomes imminent.

IMPLEMENT A BYSTANDER REPORTING PROGRAM

Individuals who recognize concerning behaviors must have multiple avenues available to report it. Reporting concerning behavior should be seen as a collective responsibility, and organizations should strive to make bystander reporting part of an overall safe and positive work climate. It is also important that employees feel confident in reporting without fear of retaliation or punishment. While all workplaces should have a means to collect information about concerning behavior, the reporting mechanisms used by employees may vary based upon a variety of factors, such as the organization size, type, industry, or other aspects of the work environment. For instance, a reporting option that works for a small food service business may not be an appropriate solution for a large multinational corporation.

When choosing the appropriate reporting solution, organizations must consider the resources available, the needs across their workforce, and the unique context of their environment. ***Improving School Safety Through Bystander Reporting: A Toolkit for Strengthening K–12 Reporting Programs*** (2023)[12] is a joint publication produced by the U.S. Secret Service and the Cybersecurity and Infrastructure Security Agency (CISA) which outlines strategies for establishing and enhancing reporting programs. While this toolkit was written primarily for K–12 school audiences, the principles presented therein are research-based and are broadly applicable to reporting mechanisms established in other environments, including workplaces. Best practices for developing workplace reporting systems include the following:

Promote multiple reporting methods to improve accessibility. Organizations should offer simple and accessible means for individuals to share concerns. Reporting can be accomplished through a variety of avenues. Smaller organizations with few employees may consider using a dedicated email address where employees can express concerns, while larger organizations may need to adopt more sophisticated means of collecting reports, such as a phone hotline, a mobile application, and/or an online form via the organization's website. Offering multiple avenues for reporting can increase the likelihood that employees will share their concerns, thereby enhancing the opportunity for organizations to take appropriate action. Training and awareness campaigns should be utilized to instruct relevant stakeholders on how and what to report. This can include using posters, brochures, online resources, and training events (see Step 8).

Set operating hours that improve availability. Reports can be received at any time. Every member of the BTAM team should have the capability to view received reports and should automatically be notified of incoming reports, even outside of normal operating hours, if possible. Some organizations utilize partnerships with law enforcement agencies or a third-party dispatch center that has 24/7 availability to receive and process reports outside of work hours. The more frequently reports are checked, the faster teams can respond to concerns.

Consider an anonymous or confidential reporting option. Some employees may be hesitant to report behaviors and communications of concern in the workplace due to fear of retaliation. Anonymity and confidentiality can encourage reporting throughout an organization by making employees feel more confident that their privacy will be protected and that they will be safe from retaliation. In some cases, organizations may be able to establish two-way messaging that allows follow-up communication without requiring an individual to disclose their name. Other options include anonymous or confidential reporting forms, hotlines, or mobile applications that safeguard the reporter's identity.

Field reports in a timely and transparent manner. BTAM teams should ensure reports are routed to the correct party so appropriate action can be taken in a timely manner. Transparency in communications with stakeholders, including describing what actions have been or will be taken to address concerns, can be an important strategy to build trust and credibility in the BTAM process.

USING TECHNOLOGICAL TOOLS TO IDENTIFY CONCERNING ONLINE ACTIVITY

Some organizational BTAM teams partner with cybersecurity and IT professionals to incorporate specialized technological tools to identify threatening or concerning behavior while an employee is using the organization's network or devices. Such tools are autonomous and continuous, and they can be used in conjunction with human monitoring to detect and prevent risk of harm.[13] Cybersecurity and IT professionals may set up mechanisms to alert the BTAM team to anomalous digital behaviors, including employees who visit blocked or forbidden websites on multiple occasions or log onto their devices at unusual times. These tools can also be used to perform keyword monitoring of browser searches or internal communications, flagging keywords related to hate speech, weapons, violence, or concerning, inappropriate, or extremist language. BTAM teams can use these tools to proactively identify concerning behaviors and intervene.

PROCESS AND TRIAGE REPORTS

It is important to establish how reports of concern will be initially processed upon receipt. The approach may vary based upon the organization's characteristics, including organizational size, staffing, and other factors. For example, small organizations may have reports sent directly to the BTAM team for screening and assessment. However, large organizations that receive many reports can utilize a more complex triaging process in which reports undergo a preliminary evaluation of their imminence and relevance to the BTAM team to determine how the report will be routed and assessed.

Reports should be received by trained individuals who are familiar with the BTAM process and understand that even an isolated report may be indicative of a larger risk. In some cases, one component of the organization may be better equipped to evaluate and/or address a concern than another component, and these differences should be considered when determining how reports of concern will be processed.

Once a report is received, an initial screening should be completed. During the initial screening, three determinations should be made about the report:

Is the report describing an emergency? Reports that describe emergency situations, such as a terminated employee brandishing a weapon on site, are not appropriate for a BTAM and should instead prompt an immediate call to security, emergency dispatchers, local law enforcement, or other appropriate officials capable of a rapid response.

Is the report credible? The report should appear to be accurate, be submitted in good faith, and include specific details about the individual of concern and the nature of the threat or concern. If the BTAM team is unsure about the credibility of a report, the team should commence additional information gathering until a determination can be made.

Is the report actionable? The report should contain enough details about the situation that elicited concern to facilitate further investigation and should be relevant to the purpose and scope of the BTAM program.

Most non-imminent reports that are deemed credible and actionable during an initial screening should be routed to the appropriate party, usually the organizational BTAM team, for inquiry and assessment (see Step 5). Other cases may require no further action from the BTAM team, but they may be appropriate for other services or systems. This may occur, for example, when reports are submitted regarding issues that are outside the purview of the BTAM team's responsibilities (e.g., requests for reasonable accommodations). In these instances, the report should be routed to the appropriate party, the reason for referral should be documented, and the records should be preserved based on the organization's records retention policies.

THREATS TO EXECUTIVES

Due to the high visibility of their positions, executives and high-ranking officials can attract a lot of attention from the general public. This visibility can present unique safety challenges when individuals harbor grievances against an organization and focus their hostilities on the organization's leadership, making executives vulnerable to stalking, harassment, and targeted attacks.

How prevalent are threats to executives?
Executives and high-ranking officials have experienced a gradual increase in threats of violence over the past decade, with sharper increases in recent years. A report published in 2025 by the Security Executive Council and Mercyhurst University examined 424 incidents and found that physical and cyber incidents targeting executives have doubled since 2024, resulting in record numbers.[14] Further, a 2026 security report found that 42% of over 2,000 chief security officers who were surveyed reported that the threat of violence toward executives had increased within the previous two years.[15]

What actions can organizations take to prevent violence?
The guidance in this publication is intended to help prevent targeted workplace violence from impacting all personnel, including executives. However, due to the unique characteristics of threats to executives, some organizations use additional strategies to protect high-ranking officials. These strategies can include:

- **Digital monitoring.** Dedicated analysts routinely monitor digital platforms, including social media, to assess and respond to threats, harassment, or other concerning behaviors targeting executives.
- **Close protection teams.** Specially trained security teams provide physical protection for executives while they are at home, in the office, or during travel.
- **Travel advances.** Teams of analysts and security personnel gather reliable intelligence and coordinate security and transportation logistics before an executive takes a domestic or international trip. During the trip, the team provides real-time support.
- **Residential security.** Some organizations implement physical security enhancements at an executive's home to bolster protective efforts. These enhancements can include surveillance systems, alarms, access controls, and on-site security staff.[16]

STEP 5: GATHER INFORMATION TO ASSESS FOR RISK

When actionable reports of concerning behavior are received, BTAM teams must conduct a comprehensive evaluation of the risk posed by the individual. To accomplish this, BTAM teams should conduct a preliminary inquiry and/or full assessment to systematically gather information to develop a comprehensive understanding of the thinking and behaviors of the individual of concern.

The purpose of the assessment phase in BTAM is to determine whether an individual poses a risk of harm to themselves or others. To make this determination, BTAM teams should use a fact-based process to gather information from diverse sources, identify key details about the individual's thinking and behavior, and consider the context of the individual's situation and unique circumstances. In workplace settings, this process may entail gathering information from individuals and systems both inside and outside of the organization, then piecing together a comprehensive picture of the individual's behavior and life circumstances so an informed and reliable assessment of risk can be made. Gathering information can be accomplished using a phased procedure beginning with a preliminary inquiry and, when appropriate, conducting a full assessment. BTAM teams should utilize the *Systems Approach* and explore relevant *Assessment Themes,* both described later in this step, when gathering information and making a determination of risk.

THE SIGNIFICANT ROLE OF WORKPLACES IN PREVENTION

NTAC's research has shown that most attackers exhibited behaviors that elicited concern in others prior to their attacks, and these behaviors were observed among a variety of systems. In *Mass Attacks in Public Spaces: 2016 – 2020* (2023), NTAC found that the workplace was the most common formal setting in which concerning behavior was observed. This finding highlights the key role workplaces can play in early detection.

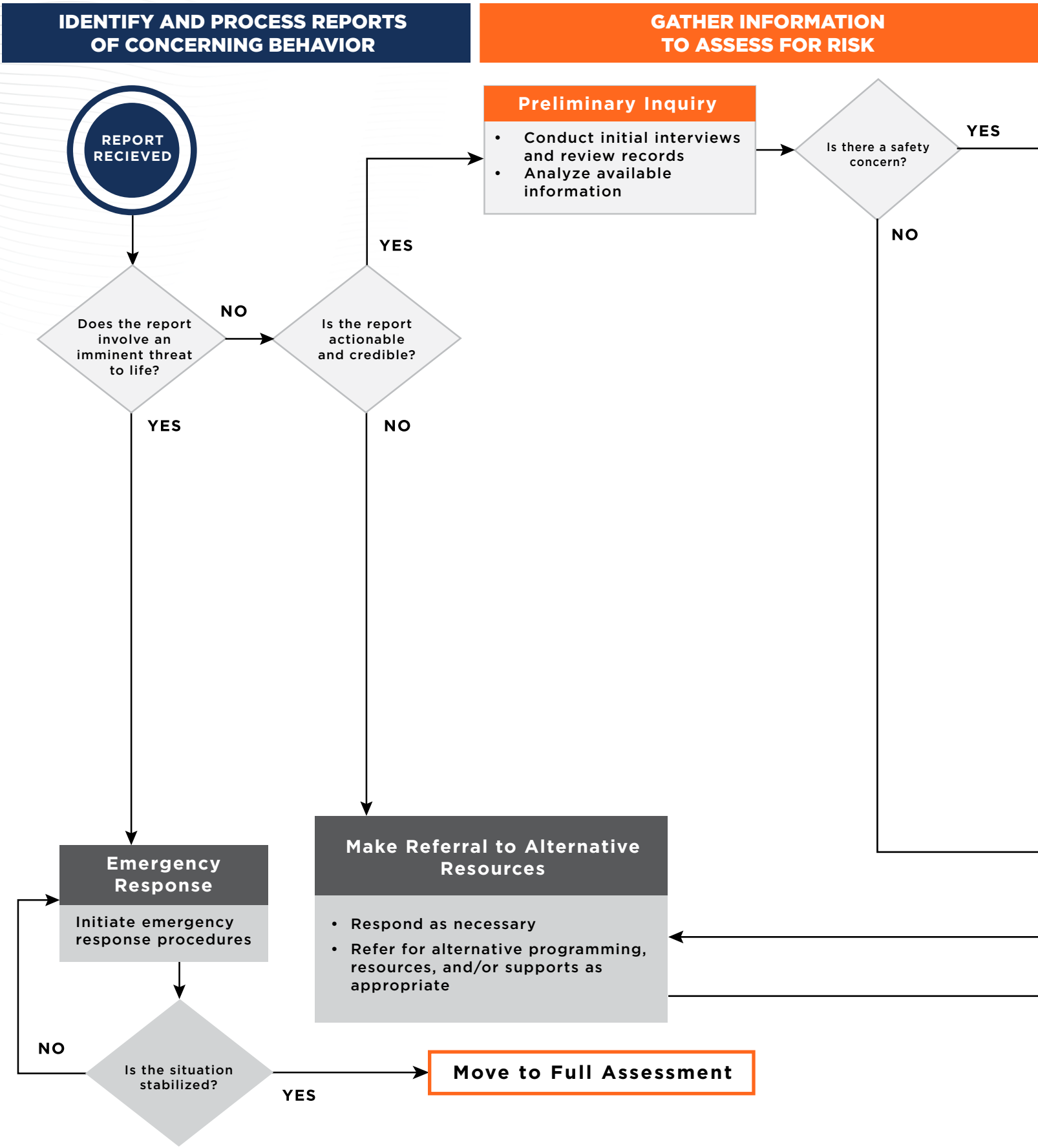
Figure 9 on the following pages illustrates a potential pathway for a report of concern from initial intake to case closure.

FIGURE 9

BTAM Case Management Process

**IOC refers to an individual of concern.*

SCAN QR CODE OR VISIT SECRETSERVICE.GOV/NTAC TO DOWNLOAD



DEVELOP RISK MANAGEMENT STRATEGIES

Full Assessment

- Conduct interviews and review records
- Use the Systems Approach to gather information
- Explore relevant Assessment Themes
- Analyze available information

Does the IOC* pose a risk of harm to self or others?

YES

NO

Implement Risk Management Strategies

- Develop or refine an individualized management plan
- Document and implement strategies as appropriate

Evaluate

- Examine whether the case management plan is having the intended impact
- Adjust and update the case plan as needed

Does the IOC* pose a risk of harm to self or others?

YES

NO

Could the IOC* benefit from other resources?

NO

YES

Close BTAM Case

- Document all actions, findings, and determinations
- Follow record retention protocols
- Share information as appropriate

CASE CLOSURE

PRELIMINARY INQUIRY VS. FULL ASSESSMENT

One early and necessary determination in the BTAM process is distinguishing between the need for a preliminary inquiry or a full assessment when responding to reports of concerning behavior in the workplace. This tiered approach ensures that resources are allocated appropriately and that every report receives an appropriate individualized response.

PRELIMINARY INQUIRY

Following initial triage (see Step 4) of any actionable report of concerning behavior, a **preliminary inquiry** serves as the minimum level of response. Preliminary inquiries are limited in scope and designed to quickly gather enough information to establish an understanding of the concern and the context needed to determine next steps. This process may involve conducting interviews with the reporting person(s), the individual of concern, and others who are directly familiar with the individual or situation, such as work supervisors or HR professionals. Information for a preliminary inquiry may also come from additional sources, for example, a review of the individual's publicly available social media, as needed. The objective of the preliminary inquiry is to establish enough context to assess whether the case should be closed or elevated to a full assessment. If the preliminary inquiry reveals that the individual may pose a risk of harm or that more information is necessary to make that determination, the BTAM team should proceed with a full assessment.

FULL ASSESSMENT

A full assessment is conducted when:

- the reported concern is objectively concerning enough to bypass a preliminary inquiry and move immediately to a full assessment;
- the preliminary inquiry reveals a substantial concern; or
- the preliminary inquiry alone did not yield enough information to make an assessment of risk.

A **full assessment** involves gathering more detailed information from more diverse sources, including a broader group of the people and systems with whom the individual of concern has interacted. A full assessment typically involves multiple interviews, records checks, reviews of publicly available social media, and analysis of employer-issued electronic devices. Gathering this information enables the BTAM team to gain a reasonable and articulable understanding of the risk posed, identify factors specific to the individual that increase or decrease risk, and determine effective strategies to intervene and prevent a potential escalation to violence.

THE SYSTEMS APPROACH

The effectiveness of the BTAM team depends upon its ability to gather substantive information from the people and systems with whom the individual of concern interacts. To achieve this, the U.S. Secret Service pioneered the ***Systems Approach***—a process of gathering information from various community systems in order to provide a

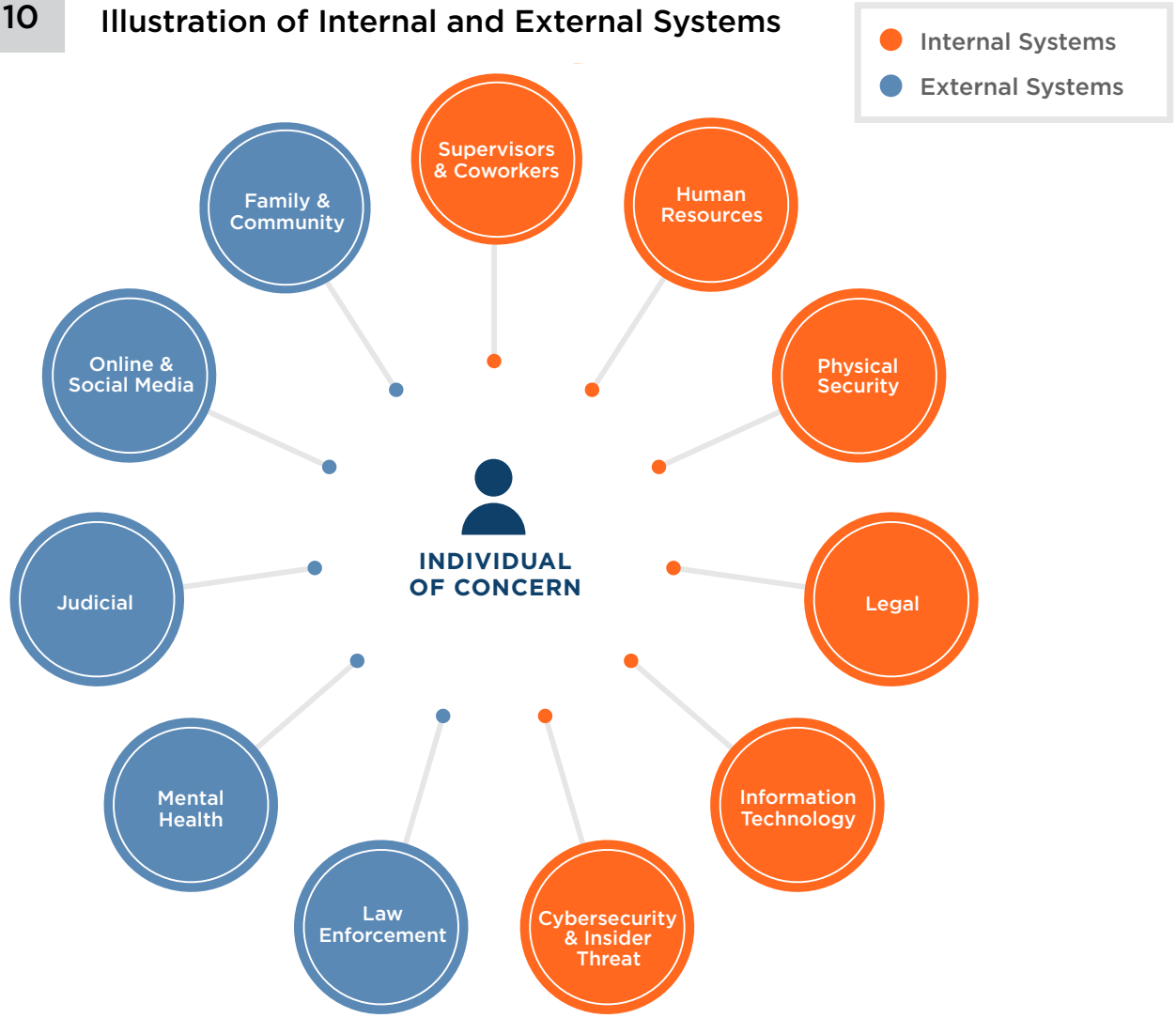
SYSTEMS APPROACH:

A process of gathering information from various community systems in order to provide a comprehensive and reliable assessment of an individual's thinking and behavior.

comprehensive and reliable assessment of an individual's thinking and behavior. Systems in a workplace can be internal components, such as security or human resources departments, or external community partners, such as law enforcement and mental health providers. The Systems Approach allows BTAM teams to collect and synthesize pieces of information that may otherwise be siloed. In many cases, attackers had demonstrated concerning behavior at work, at home, and online before their attack, but no program existed to examine these behaviors collectively. By utilizing the Systems Approach, BTAM teams can identify and synthesize information from numerous sources to make a holistic determination about the risk an individual of concern may pose. This approach can also be an effective tool for identifying potential risk management strategies (see Step 6).

Figure 10 illustrates the Secret Service's Systems Approach adapted for workplaces. The center of the diagram represents the individual of concern who is the subject of the assessment. The circles surrounding the individual of concern represent some of the workplace and community systems that may provide important behavioral and contextual information about the individual to inform the BTAM process. In this diagram, orange circles represent *internal systems* to which a BTAM team should have immediate access, while blue circles represent *external systems* outside of the workplace.

FIGURE 10 Illustration of Internal and External Systems



Although the general method for gathering information using the Systems Approach remains the same for all cases, the specific systems used may differ from case to case. For instance, an organization's assessment of a current employee may look different and may leverage different sources of information compared to the systems used when assessing a customer.

USING THE SYSTEMS APPROACH

The fictional examples described below highlight how different systems may be leveraged depending on the unique characteristics of a case.

EXAMPLE 1 - EMPLOYEE: Employees at a software company submit a report of concern to the BTAM team about a colleague who is making increasingly agitated statements. During their assessment, the BTAM team uses the Systems Approach to identify several concerns about the employee: his supervisor reports a sharp decline in the employee's recent performance and demeanor, his coworkers report that he has claimed he might "snap" if things don't improve at work, and HR reports that a coworker recently submitted complaints about the employee's rude and combative nature. The BTAM team conducts an interview with the employee and discovers that he is going through a difficult separation from his spouse and has had trouble adjusting to this change, which the employee's brother confirmed during a phone call. Through coordinated outreach between the BTAM team, his supervisor, and HR, the employee has his workload reduced temporarily and is referred to the company's EAP so that he may receive counseling and support.

EXAMPLE 2 - CUSTOMER: A major retail outlet has a frequent customer with a history of disruptive and concerning behaviors who recently made posts on social media alluding to something bad happening to the store. The BTAM team uses the Systems Approach to gather information through interviews with employees from the store, direct the company IT department to further review the individual's publicly available social media posts, and coordinate with law enforcement to conduct a consensual interview with the individual regarding the social media posts. The BTAM team determines that the individual presents a low risk for physical harm but a high risk for causing disruption at the store. The BTAM team works with local law enforcement to issue the customer a no trespass order from all physical store locations, while offering him discount codes for online shopping through the store's website.

INTERNAL SYSTEMS

Internal systems are systems within the organization itself. While the amount of contact or exposure to an individual of concern may vary from case to case, these systems are almost always relevant when assessing and managing an individual of concern who is currently, or has previously been, employed by the organization. For employees, leveraging organizational systems will often be sufficient to assess and manage the risk posed. Internal systems can also have relevant information about other individuals of concern, including customers, clients, visitors, or members of the broader public. For instance, a retail organization conducting a behavioral threat assessment on a frequent and troublesome customer may get valuable insight into the individual's background and behaviors by speaking with their physical security professionals with whom the disruptive customer has interacted.

To accurately assess risk, BTAM teams should gather and examine information from a variety of internal systems that provide insight into concerning and/or mitigating information regarding the individual of concern, including:

Supervisors and Coworkers. Employees who interact with the individual of concern may offer observations and information about past interactions, perceived behavioral changes, and indicators of escalating stress or hostility.

Human Resources (HR). HR professionals may offer information pertaining to the individual's employment history, work performance, behavioral conduct, grievances, conflicts, disciplinary actions, accolades, and attendance records.

Physical Security. Physical security personnel may offer behavioral observations, details about security incidents, witness statements, building or facility access logs, and security footage.

Legal. Legal personnel may offer records of legal filings or complaints—such as claims of harassment, restraining orders, and prior violent incidents—and legal rights or protections.

Information Technology (IT). IT may assist with access to system records, including login history, email communications, and internet usage.

Cybersecurity and Insider Threat. Cybersecurity and insider threat professionals may offer data from user activity monitoring, including online network or electronic device activity (e.g., emails, file downloads, social media usage), and information about anomalous digital behaviors, such as unauthorized or failed access attempts to restricted systems or files.

INSIDER THREAT PROGRAMS

Insider threat programs are designed to detect risks from trusted insiders, such as employees or contractors, who may intentionally or unintentionally cause harm. These programs typically focus on areas such as unauthorized access to sensitive data, sabotage, fraud, and misuse of systems, whereas BTAM programs focus on violence against individuals in the workplace.

However, both insider threat and BTAM programs are specifically designed to detect early behavioral red flags, aggregate data from multiple sources, and facilitate cross-functional collaboration. These similarities make insider threat programs well-positioned to support BTAM teams in identifying and mitigating risk before it escalates to violence. Collaboration and partnership between these programs can enable each to perform their functions more effectively and ultimately help protect workplaces from targeted workplace violence and other potential risks.

EXTERNAL SYSTEMS

External systems are systems outside of the workplace that may be of particular importance when assessing and managing individuals who are not directly affiliated with the organization (e.g. customers, visitors). Some employees of concern, particularly those engaging in highly concerning behaviors, may also warrant the use of external systems to gather information when assessing risk. This highlights the importance of preemptively establishing collaborative relationships with those outside the organization (see Step 1). BTAM teams may seek to gather and examine information from a variety of external systems, including the following:

Law Enforcement. Coordination with law enforcement partners can be critical for organizations, particularly in highly concerning cases where violence or criminal behavior is possible, or in cases involving individuals who are not associated with the organization (e.g., customers). Law enforcement agencies possess the legal authority, training, and operational protocols needed to safely engage with individuals outside the organization, ensuring that privacy rights are protected and that investigative activity does not escalate the situation or expose the workplace to liability. Organizations may coordinate with law enforcement to serve or enforce a protective order or to request a welfare check to assess an individual's well-being at home.

Judicial. Publicly available court records (e.g., criminal charges, convictions, protective orders, civil lawsuits, eviction filings, bankruptcy declarations), which can be found on many judicial and governmental websites, can provide relevant context about an individual's legal history or other stressors. While these records alone do not indicate a threat, when reviewed in context with other stressors or criminal behaviors present in the individual's background, they can help BTAM teams identify a history of aggression, violence, or signs of instability or distress.

Mental Health. Community mental health partners can be valuable assets at nearly any stage of a behavioral threat assessment. These professionals can provide assistance in a consultative capacity, leveraging their professional expertise to assess the risks posed by an individual or situation, particularly in cases where individuals may be experiencing mental health crises. These partners can offer valuable insight into potential symptoms and diagnoses, help BTAM teams understand unusual patterns of behavior, and identify avenues for evaluation and treatment, as discussed in the next step of this guidance.

Online and Social Media. Publicly available posts on social media, forums, or content-sharing platforms can reveal grievances, intent, or interest in violence. Social media content can also contain indicators that an individual is in crisis (e.g., expressions of hopelessness, desperation, pleas for help), which could warrant further assessment.

THE VALUE OF OPEN-SOURCE EXPERTISE

Including a team member with expertise in open-source investigations can significantly enhance a BTAM team's ability to identify digital and online indicators of concern. These team members should be trained to ethically and efficiently find, gather, and analyze publicly available open-source information (e.g., social media accounts, message boards, personal websites) that may not appear in other systems.

Family and Community. Members of the community (e.g., family, friends) may offer critical insight into an individual's behavior and current circumstances, especially during times of crisis. Seeking to interview members of the community will typically occur by requesting the support of law enforcement and only in serious or high-risk situations. If an individual of concern is a current or former employee, emergency contacts listed in their personnel file may help BTAM teams identify family and community members who have personal information about the individual.

ASSESSMENT THEMES

In ***Behavioral Threat Assessment Units: A Guide for State and Local Law Enforcement to Prevent Targeted Violence*** (2024),[17] NTAC presented the 20 Assessment Themes that have been established by 25 years of NTAC research and the Secret Service's unique operational expertise in violence prevention. ***Assessment Themes*** characterize common patterns of thinking and behavior found in the background and behavioral history of individuals who have engaged in past acts of targeted violence. Assessment Themes can also help identify relevant protective factors for an individual of concern, which can reduce an individual's risk by bolstering their capacity to cope with challenges. While BTAM teams gather information from the internal and external systems relevant to the individual of concern, these Assessment Themes should guide the team's evaluation of the individual's behaviors, personal circumstances, and relevant environmental factors which may increase, decrease, or contextualize concern.

ASSESSMENT THEMES:

Areas of inquiry that, when explored, will provide a contextual understanding of an individual's mindset, behavior, and circumstances that will allow a BTAM team to assess if the individual poses a risk of violence.

Importantly, Assessment Themes are **not intended to be used as a checklist** to predict who will engage in violence. Instead, these themes **provide a structured framework to guide the gathering and integration of information** about the individual of concern. This framework helps BTAM professionals look beyond isolated incidents and evaluate behavior in a broader context. This approach ensures decisions are not made based on subjective judgments or initial impressions, but instead on a comprehensive and methodical review of relevant information. Additionally, these themes allow BTAM teams to distinguish between situational behaviors, such as temporary frustrations or poor communication, and more persistent, escalating patterns of concern.

There are three relevant categories of Assessment Themes: contextual themes, behavioral themes, and summative themes. Each category is described on the following pages.

CONTEXTUAL THEMES

Contextual themes represent significant elements of an individual's personal circumstances and surroundings that may impact their thinking and behavior. Some of these contextual themes have their own body of existing research examining their impact on an individual, and prior NTAC research has found that many past attackers had substantial negative experiences related to these contextual themes as well. Gathering both positive details (e.g., caring and supportive family) and negative details (e.g., familial discord and violence) about these factors will establish the context of past, present, and impending circumstances within which the individual of concern is operating, and this will inform the BTAM team's risk management strategies.

STRESSORS

Significant setbacks, losses, and other life challenges that may be acute (e.g., romantic breakups) or chronic (e.g., ongoing medical conditions). Stressors can be experienced across several life domains, including family/romantic relationships, social interactions, work or school environments, personal health, legal actions, and other identified areas. Specific examples include being bullied or harassed by others, financial instability, job loss, divorce or child custody issues, and failed life aspirations.

HOME LIFE

Family dynamics or home environments that negatively impact an individual, including family discord, abuse, drug use, criminality, domestic violence, mental/physical health concerns, death, and dissolution of relationships. Conversely, positive home life factors may include supportive families, healthy relationships, and other dynamics that could support intervention strategies to mitigate risk.

MENTAL HEALTH

Current or previous history of mental health symptoms that negatively impact the individual, particularly when left untreated, including paranoia, delusions, hallucinations, depression, and suicidality. Mental health history may or may not include prior formal diagnoses, hospitalizations, and treatment (e.g., prescription medication).

CRIMINAL HISTORY

A history of criminal behavior identified in formal records, including arrests, convictions, and other legal actions. Criminal history may also include other criminal behavior and contacts with law enforcement and the courts that have not resulted in official legal actions. Outside of formal records, criminal behavior may be identified during the assessment through interviews with family, friends, coworkers, classmates, and others familiar with the individual.

INTERPERSONAL DIFFICULTIES

A pattern of strained or conflicted relationships with family members, romantic partners, friends, coworkers, classmates, neighbors, or other members of the community. Interpersonal difficulties may include an inability to form or sustain positive relationships with others due to the individual's inappropriate or concerning behaviors.

LACK OF CONSEQUENCES

A pattern of engaging in criminal or inappropriate behavior for which the consequences were either absent or not commensurate with the behavior. Examples of past behaviors that may not have received appropriate consequences could include threatening communications, domestic violence, physical/sexual assaults, inappropriate touching of others, stalking, and harassment.

BEHAVIORAL THEMES

Central to assessing whether an individual poses a risk of targeted violence is understanding the nature of concerning behaviors commonly observed in previous attackers. While the presence of these **behavioral themes** alone cannot predict if an individual will become violent, it will inform the final assessment and management strategies employed by BTAM teams. For example, if an assessment reveals an individual is fixated on past attackers, has grown increasingly isolated, and has posted concerning violent content on social media, the BTAM team will need to develop the appropriate strategies to manage the risk the individual may pose toward the workplace.

CONCERNING OR THREATENING COMMUNICATIONS

Any violent, threatening, or disturbing communications which may be conveyed verbally (e.g., in-person or via phone), in writing (e.g., journals or drawings), electronically (e.g., text messages or emails), online (e.g., websites, blogs, or social media), or by other means. The content of the concerning communications may reveal information on threats, grievances, violent intention, feelings of hopelessness/suicidality, obsessions, paranoid thinking, or a fascination with violence or weapons.

INTEREST IN VIOLENT TOPICS

An unusual or excessive interest in weapons, violence, gore, prior attacks, notorious killers, or other concerning topics. Fascination with weapons and violence can be demonstrated in a variety of ways, including stockpiling or manufacturing weapons, being described as obsessed with weapons, consuming or producing violent or graphic media, and writing stories or lyrics indicating a desire to harm others. Particular concern should arise if the individual demonstrates an idolization of or desire to emulate past attackers.

HISTORY OF VIOLENCE

Prior acts of physical violence against people, animals, or property that may appear in criminal records or may be observed or experienced by others, including physical and sexual assaults, domestic/family violence, animal cruelty, menacing behaviors, or arsons. A history of violence may reveal signs of an escalation in aggressive behavior, for example, moving from property crimes to crimes against persons.

STALKING, HARASSING, OR BULLYING

A pattern of conduct that willfully and maliciously causes another to feel bullied, stalked, persecuted, threatened, injured, or attacked. The victim of this behavior may or may not have a pre-existing relationship with the individual of concern. Examples of victims with a pre-existing relationship to the individual include romantic partners, family members, coworkers, classmates, doctors, attorneys, or neighbors, while those without a prior relationship may include elected officials, government employees, or celebrities.

EXTREME BELIEFS

Extreme ideological, political, or conspiratorial beliefs that advocate hate or violence, form the basis of an individual's worldview, or significantly influence an individual's daily life. Extreme beliefs may be based on distortion of facts (e.g., conspiracy theories) or may advocate distrust, hatred, or the use of violence targeting others based on biases against a particular race, religion, national origin, sexual orientation, gender, or gender identity.

BEHAVIORAL THEMES *(continued)*

FIXATIONS

Intense or obsessive preoccupations with a person, event, activity, or belief, to the point where they negatively impact aspects of an individual's life. Fixations often carry an angry or emotional undertone and may be evidenced through an individual's extreme beliefs, grievances, interest in violence or weapons, and stalking or harassing behaviors.

BEHAVIOR CHANGES

Changes in behavior observable to others, including notable shifts in mental, social, occupational, physical, or interpersonal functioning. This may be evidenced through changes in mood, appearance, or hygiene; withdrawing or isolating from others; new or increased substance use; sudden aggressive, violent, or threatening behavior; changes in work or school attendance or performance; signs of depression or paranoia; or other uncharacteristic actions that demonstrate a distinct change from an individual's baseline behavior.

DESPERATION OR DESPAIR

Feeling hopeless, despondent, desperate, or out of options. An individual's inability to perceive an improvement in their situation may lead to feelings of extreme distress, depression, frustration, and the perception that violence is the only option to cope with their circumstances.

INTENSE ANGER OR AGGRESSION

A pattern of intense or escalating anger or aggression that is observed through the individual's behavior, communication, or reported feelings. This may be marked by impulsive angry outbursts, significant overreaction to circumstances or events, or frequent episodes of verbal or physical aggression directed at others.

INCONSISTENCY

Evidence of unusual inconsistencies in an individual's communications and behaviors that may occur across the various community systems in their lives, including how they behave at work, home, or school, or in social or romantic contexts. When inconsistencies are found, these may be indicative of efforts to conceal violent intentions or behavior.

PLANNING AND FINAL ACTS

Specific steps taken to prepare to carry out an act of violence, including researching, visiting, or following potential targets; researching, manufacturing, acquiring, or practicing with weapons; documenting preparations for an attack through hit lists, to-do lists, maps, or manifestos; researching prior attacks and tactics; developing attack plans; researching logistical concerns; or using deceptive practices to hide activities. Individuals may also engage in final acts intended to make a statement or to prepare for their inevitable arrest or death. These acts may include drafting a last will and testament, making financial arrangements for family members, leaving farewell messages or notes, posting goodbye messages online, and selling or giving away personal possessions.

SUMMATIVE THEMES

Summative themes represent key questions that must be answered as part of an overall assessment. BTAM teams will be better equipped to make an informed assessment of risk if they have identified what is, or could be, motivating someone to become violent. They will also need to understand if the people who know or have had contact with the individual have been concerned, especially if their concern is related to safety. Lastly, BTAM teams will need to assess if the individual has the means and capability to cause harm by gathering information about the weapons the individual has access to or could potentially obtain.

ELICITED CONCERN IN OTHERS

The individual's behaviors or communications have caused fear, alarm, worry, or distress in those who observed them. Particular attention should be paid to whether others are in fear for their safety as a result of the individual's behavior. Family members, friends, coworkers, neighbors, law enforcement, mental health professionals, and others may have been concerned about an individual's demeanor, mental well-being, threatening or disturbing communications, harassing or other violent behavior, obsession with weapons or violent topics, isolating or withdrawing from others, substance use or abuse, or other concerning behaviors.

MOTIVE

The reason(s) why the individual engaged in the behavior that elicited concern or brought them to the attention of the BTAM team. Motive also includes assessing the reasons that may drive an individual to carry out an act of violence. Motives may be multifaceted and include retaliating for grievances or perceived wrongs (e.g., bullying, failed romantic relationships, workplace issues); furthering ideological, bias-related, or political beliefs; acting in response to psychotic symptoms; having a desire to kill; achieving fame or notoriety; and committing suicide-by-cop.

ACCESS TO WEAPONS

Current or future ability to access weapons that could be used to cause harm, including firearms, bladed weapons, explosives, chemicals, and poisons. Access to weapons may include those that are readily available to the individual in their home, whether secured or unsecured, as well as those accessible in the homes of relatives or friends.

Figure 11 illustrates the contextual, behavioral, and summative themes that may be relevant to an assessment. Each assessment theme should be understood in the context of an individual's full background and behavioral history. Individuals of concern can exhibit characteristics or behaviors relevant to one or more assessment themes. The case example on the following page highlights some of the contextual, behavioral, and summative themes relevant to the background and behaviors of one individual who engaged in an act of targeted workplace violence.

FIGURE 11 Assessment Themes

CONTEXTUAL THEMES	BEHAVIORAL THEMES	SUMMATIVE THEMES
Stressors	Concerning or Threatening Communications	Motives
Home Life	Interest in Violent Topics	Elicited Concern in Others
Mental Health	History of Violence	Access to Weapons
Criminal History	Stalking, Harassing, or Bullying	
Interpersonal Difficulties	Extreme Beliefs	
Lack of Consequences	Fixations	
	Behavior Changes	
	Desperation or Despair	
	Intense Anger or Aggression	

CASE EXAMPLE OF ASSESSMENT THEMES

On October 18, 2017, a 37-year-old man gathered coworkers around him by calling an impromptu meeting at the manufacturing facility where he worked. He then drew a semiautomatic pistol and shot five of his colleagues in the head, killing three and injuring two others. The attacker was motivated by a ***grievance against his coworkers*** *who frequently played pranks on others at work, of which he felt he was the victim. After shooting his coworkers, the attacker proceeded to drive to two more locations, including a former workplace where he likely targeted his former boss who was not there, and another location where he shot and injured a business owner he knew.*

Prior to his attack, the attacker experienced several stressors in his life, including ***financial hardship*** and ***strained relationships*** *both inside and outside of the workplace. Three years prior to his attack, he was also a* ***victim of physical assault*** *in a parking lot. In the aftermath of his assault, he was known to be* ***paranoid****, believing others were searching for him or out to get him. To protect himself, the attacker* ***purchased a firearm illegally*** *due to* ***felony convictions*** *on his criminal record and reportedly kept the weapon with him at all times.*

Additionally, the attacker had a history of threatening and concerning behaviors in his previous jobs and was terminated from these positions due to his ***aggressive behavior****. On one occasion, he was arrested for* ***assaulting a coworker*** *after he put the coworker in a chokehold, dragged him outside, and threw him to the ground so hard that the coworker lost consciousness. In a separate incident six months before the attack, the attacker was* ***fired from a previous job*** *after initiating a* ***physical altercation*** *with his manager because he was not granted a raise that was previously discussed.*

The attacker began working at the manufacturing facility about four months before the attack. He was known to act in a paranoid, hostile, and argumentative manner and ***harassed his coworkers****. This included accusing non-English speakers of gossiping about him, using derogatory language toward them,* ***threatening to kill them****, and* ***assaulting coworkers*** *he felt disrespected him. These behaviors were noticed by others in the workplace, and* ***coworkers reported their concerns*** *about the attacker's behaviors to management and requested help. However, management reportedly refused to intervene because the attacker was a good worker, and no action was taken.*

Contextual Themes

Stressors
- Financial hardship
- Fired from previous job
- Victim of physical assault

Interpersonal Difficulties
- Strained relationships

Mental Health
- Paranoid

Criminal History
- Felony convictions

Behavioral Themes

Intense Anger or Aggression
- Aggressive behavior

History of Violence
- Assaulted coworkers
- Physical altercations

Stalking, Harassing, or Bullying
- Harassed his coworkers

Concerning or Threatening Communications
- Threatened to kill coworkers

Summative Themes

Access to Weapons
- Purchased a firearm

Elicited Concern in Others
- Coworkers reported concerns

Motive
- Grievance against his coworkers

MAKE AN ASSESSMENT OF RISK

As information is gathered from interviews, records, and other sources, the BTAM team must assess whether an individual of concern poses a risk of violence. Using the information gathered, the BTAM team will seek to answer this central question: **Does the individual of concern pose a risk of violence at this time?** The BTAM team should make this determination by considering all information obtained using the *Systems Approach* and considering relevant *Assessment Themes* and other situational factors. If the BTAM team determines that the individual of concern does pose a risk of harm, then the BTAM team should take steps to intervene and manage the risk posed (see Step 6).

Some BTAM teams might prefer to classify their assessments into levels of risk (e.g., low risk, medium risk, and high risk) for case prioritization and management. If doing so, BTAM teams should ensure that each classification level is clearly defined and articulable (e.g., clarifying the distinction between low and medium risk) to avoid confusion and inconsistencies across assessments. The BTAM team's protocols should allow for the team to deviate from the ascribed level of risk, if needed, based on any unique circumstances identified during the assessment. Protocols should also allow for implementing risk management resources in all cases, including those deemed low risk.

Assessing risk is a dynamic and continuous process. The BTAM team should routinely assess any changes or new information that may increase, decrease, or contextualize the risk of harm posed by the individual of concern. Even if the individual does not appear to currently pose a risk of violence, BTAM teams may decide to implement risk management strategies to support the individual's well-being and prevent a potential escalation to violence.

STANDARDIZED ASSESSMENT FORMS

Organizations should develop standardized forms to provide structure and consistency in documenting the BTAM process, including the following:

- **Preliminary inquiry forms** to capture the nature of the report, sources of information that must be reviewed, initial findings, and a determination of action (e.g., whether no further action is needed or a full threat assessment is required).
- **Interview questionnaires** to gather background information about the interview subject, details about the behaviors of concern, the context for these behaviors, information relevant to Assessment Themes and protective factors, and other details.
- **Assessment forms** to document sources tapped when gathering information (e.g., social media, employment records), information relevant to Assessment Themes and protective factors, and final findings and determination following the complete assessment.

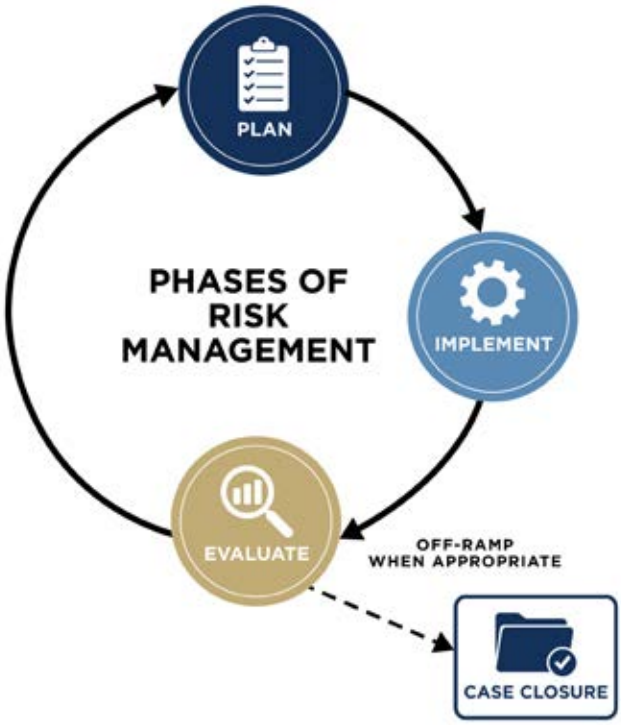
STEP 6: DEVELOP RISK MANAGEMENT STRATEGIES

When BTAM teams determine that an individual of concern poses a risk of harm to themselves or others, they must take appropriate action to reduce the risk of violence. The risk management process is dynamic, spanning multiple phases. The process should be tailored to address the unique characteristics of the individual of concern and their environment.

Using the information gathered during an assessment, BTAM teams should develop a plan to manage any risk posed by the individual of concern. BTAM teams should adopt a phased approach to continually assess risk and need, identify and implement appropriate risk management strategies, and monitor the impact of these interventions until case closure is appropriate.

PHASES OF RISK MANAGEMENT

The ***risk management*** process has four central phases: planning, implementation, evaluation, and case closure. In some cases, these phases may occur in a linear order. In other cases, the risk management process may be more dynamic whereby some phases occur concurrently, some phases are revisited, and/or some are initiated before a prior phase is ended.



Planning. During this phase, the BTAM team develops a case management plan for the individual of concern. This case management plan must be tailored to the individual and their unique circumstances and environment, and should identify specific goals and strategies to reduce their risk of harm to themselves or others. This plan should account for the concerning and mitigating factors identified during assessment.

Implementation. Once the case management plan has been established, it must be put into action. Case management strategies vary but can include making referrals for services and supports, monitoring an individual's electronic activities, placing an under-performing employee on a performance improvement plan, or encouraging a concerning individual to engage in more prosocial interests, such as hobbies or social clubs. More information on risk management strategies is described below.

Evaluation. During this phase, the BTAM team should check in with the individual of concern and/or relevant partners to determine whether risk management strategies are having the intended impact. The BTAM team should also consider whether the individual is complying with interventions, engaging with programming, and exhibiting any changes in mood, mental state, or behavior. If appropriate, the BTAM team should adjust the case management plan and implement revised strategies until the individual is no longer determined to pose a risk of harm to themselves or others.

Closure. Closure occurs when the BTAM team determines that an individual of concern no longer poses a risk of harm to themselves or others. The decision to close a case should involve all relevant stakeholders, including the BTAM team and organizational leaders. BTAM teams should be able to articulate the rationale for closing a case, document the decision, and conduct a check-in with relevant stakeholders, including the individual of concern, as deemed appropriate, to ensure no concerns return and no new concerns arise.

Throughout each of these phases of the risk management process, the BTAM team should account for relevant elements of effective risk management, which are described in detail below.

ELEMENTS OF EFFECTIVE RISK MANAGEMENT

Specific risk management strategies used during the BTAM process should be informed by the four foundational elements (see **Figure 12**): (1) address factors of concern and promote positive factors, (2) redirect potential motives for violence, (3) create a situation less prone to violence, and (4) utilize the Systems Approach for management.

ADDRESS FACTORS OF CONCERN AND PROMOTE POSITIVE FACTORS

BTAM teams should work to identify and address behavioral and situational factors that are objectively concerning, such as personal or workplace stressors. Management strategies for addressing factors of concern (i.e., negative factors) for employees can include additional employment support or mentoring, free or reduced-rate counseling services, bereavement assistance, and financial consultation. For external individuals of concern (e.g., customers or clients), BTAM teams can offer connections to community and social service providers, liaise with law enforcement to conduct wellness checks, and partner with the judicial system to obtain court orders (e.g., protection orders, restraining orders) when appropriate.

In addition to addressing negative factors, management should include efforts to promote positive factors (i.e., mitigating factors) in the individual's life. These can include support of the individual's personal, financial, and/or career goals, facilitation of social connections, and participation in employee resources and interest groups.

FIGURE 12 Elements of Risk Management

Address factors of concern and promote positive factors	Redirect potential motives for violence	Create a situation less prone to violence	Utilize the Systems Approach for management
Identify negative factors and create strategies to support positive outcomes.	Identify possible motivations and direct resources to address them.	Create an environment in which violence is less likely.	Collaborate with community stakeholders who can contribute.
EXAMPLES: ▪ Employment assistance ▪ Substance abuse treatment ▪ Counseling services	EXAMPLES: ▪ Address workplace grievances ▪ Intervene to stop bullying ▪ De-escalate interpersonal conflicts	EXAMPLES: ▪ Explore avenues for weapons removal ▪ Restrict access to work facilities ▪ Obtain restraining orders	EXAMPLES: ▪ Leverage organizational resources ▪ Identify counseling services ▪ Engage family for support
Address	Redirect	Create	Collaborate

REDIRECT POTENTIAL MOTIVES FOR VIOLENCE

NTAC's research on targeted violence has revealed that motives for violence are multifaceted, and individuals often have multiple identifiable motivations at once. BTAM teams should work to identify potential motivations for violence and take active steps to remove, reduce, or redirect those motives and encourage individuals to adopt more appropriate, prosocial behaviors. For instance, if an individual of concern is bullied in the workplace, the employee's supervisor, HR, and/or EAP services may work together to address and intervene with the bullying, create safeguards for reporting bullying behavior, and provide access to counseling and emotional support services. If the individual of concern is a customer who, for example, complains about financial hardship, the organization may liaise with community services to refer the customer for employment or income assistance. This creates a situation that can lead to positive outcomes for the individual as well as the workplace.

CREATE A SITUATION LESS PRONE TO VIOLENCE

Organizations must consider how to create a situation less prone to violence when developing risk management strategies. Specific strategies will depend on the organization, resources, applicable federal and state laws, and the characteristics of the situation and the individual of concern. Some strategies for creating a situation less prone to violence include changing an employee's schedule when there are conflicts among staff, restricting an individual of concern's access to a facility, engaging with local law enforcement for support, and limiting access to firearms when permitted by law and consistent with constitutional protections.

EXTREME RISK PROTECTION ORDERS (ERPOs)

ERPOs are civil court orders used to temporarily restrict a person's access or ability to purchase firearms if the person poses a risk of harm to themselves or others. As of 2026, over 20 states, the District of Columbia, and the U.S. Virgin Islands have ERPO laws (also called "red flag" laws). Modeled after domestic violence protection orders, ERPOs focus specifically on firearms access and can be requested by a variety of stakeholders, depending on the laws in the individual state. Eligible petitioners for an ERPO may include law enforcement, family members, romantic partners, and clinicians. California, Hawai'i, and the U.S. Virgin Islands have adopted legislation to also allow employers or coworkers to petition for an ERPO concerning an employee.

UTILIZE THE SYSTEMS APPROACH FOR MANAGEMENT

The Systems Approach (see Step 5) can identify risk management resources that can be leveraged to reduce the risk of violence for an individual of concern. When, how, and to what degree different internal and external systems are leveraged will depend on the individual of concern's affiliation with the organization, the unique circumstances of the individual of concern, and the resources available.

Organizations should proactively develop a resource guide for the BTAM team to use during management. The BTAM team should regularly review and revise the resource guide, which should include:

- a list of common needs and risk factors that may arise during a threat assessment;
- types of risk management strategies to address these needs; and
- resources, both internal and external to the organization, that can be leveraged to implement those interventions.

RISK MANAGEMENT STRATEGIES

Risk management strategies should be tailored to address the unique characteristics of the organizational environment and the individual of concern, and these strategies can be substantially different based upon whether the individual of concern is a current or former employee or a customer, client, patient, visitor, or otherwise unaffiliated with the workplace.

Organizations should develop standardized forms to document management plans and ensure structure and fidelity to the BTAM process. Useful forms during the management phase include the following:

Case Management Plan. This form should document the specific interventions pursued and implemented, detailed timelines for providing referrals, the person designated to monitor response and compliance with interventions, and the outcome of each referral or intervention. This management plan should be an adaptive, evolving process, and the forms created to document management should allow for changes to the plan and opportunities to review the effectiveness of the management strategies implemented.

Case Completion Form. This form should document the completion of the BTAM process. It should include a summary overview of the case and a reasonable and articulable determination for case closure.

STRATEGIES FOR EMPLOYEES

BTAM teams can lead employees toward positive outcomes by clearly communicating workplace expectations and what actions will be taken if those expectations are not met, as well as listening to the concerns of the employee and offering support for identified issues where possible.

Best practices in managing concerning behavior displayed by employees include:

Monitoring. Monitoring can include observing the employee's behavior, interactions, and communications with coworkers and clients; check-ins; tracking physical movement throughout a workplace; and monitoring online activities while on a company device or network.

Support and Assistance. Support and assistance are strategies that can often be used to address factors of concern. For example, EAPs can be integral in providing support for employees in the workplace by offering a confidential avenue to receive services for personal, financial, legal, medical, or work-related issues. In addition to EAPs, organizations can identify workplace mentors and peer support personnel to foster connections, as well as leverage external resources.

IN PRACTICE: SUPPORT AND ASSISTANCE

A retailer has an office that serves as a "one-stop shop" for resources and services, offering tailored solutions to manage risk for employees of concern. This includes worksite relocation services for employees experiencing personal or professional problems (e.g., bullying or harassment at home or at work), free mental health counseling services and mindfulness applications, financial grants, and contracted clinical psychologists for crisis intervention services. These resources are advertised to employees, so they know what is available and how to seek assistance.

EMPLOYEE ASSISTANCE PROGRAMS (EAPs)

Over 70 million workers in the U.S. have access to an EAP, according to data published in 2021 from the Bureau of Labor Statistics.[18] EAPs provide counseling and support to employees experiencing personal difficulties and are often underutilized. Organizations can offer EAPs as a resource during BTAM to connect employees in need with counseling and supportive services. EAPs can help employees reduce stress, improve coping skills, and handle difficulties they experience in their personal and professional lives.

Alternative Dispute Resolution. The assistance of mediators, an ombudsman, or other forms of dispute resolution should be used as needed to provide a neutral third party skilled in resolving conflict.

Performance Improvement Plans (PIPs). PIPs can be a useful tool for managing an employee's performance, maintaining accountability, and offering an avenue for structured support.

Safe Termination Procedures. There are times when separating an employee is necessary. While separations can be challenging for all parties involved, it is important that organizations practice safe separation strategies (see below) to mitigate the risk of violence.

Safe Separation Strategies

Regardless of whether an employee is being terminated or has resigned voluntarily, organizations should consider the following strategies to safely separate an employee:

Notify the appropriate personnel in advance. The decision to terminate an employee must be clearly communicated to relevant parties within the organization (e.g., security, IT, HR, management, legal) in advance to have the employee's access to various physical and cyber systems at the organization revoked, to have work reassigned as necessary, and to ensure the organization is following state and federal guidelines regarding termination.

Create a calm environment. Choose a safe and quiet location to conduct the meeting. Ensure the appropriate personnel for the separation are present. Establish a calm and clear tone to the conversation and avoid blaming or shaming the employee. Explain the rationale for the termination decision in a way that allows the employee to maintain their dignity.

Offer a "soft landing." Some organizations offer resources—including severance pay, a separation package, extended benefits or pensions, or mental health services—to reduce the risk of work-related grievances or retaliation. When appropriate and feasible, consider coordinating with community partners to offer services and support for the employee following separation.

Create and follow proper offboarding protocols. Establish a list of necessary actions to take when separating employees to ensure no important actions are missed. These protocols should include ensuring that server, file, and facility access is restricted, and that identification and credentials are turned in when offboarding employees. It may be appropriate or necessary to offer options for some employees to return materials via mail or scheduled pickup.

Follow safety practices. In some cases, it may be appropriate to utilize additional safety precautions. These can include conducting a separation meeting at an offsite location or via a phone or video conference, or establishing a security or law enforcement presence before, during, and following the termination procedures.

Post-separation efforts. In some cases, uncertainties or challenges may be experienced even after an employee has separated. When deemed necessary, coordinated outreach through appropriate channels may be used to evaluate, assess, and intervene with former employees to reduce the risk of violence. These strategies can include following up with an employee or their friends, family, or mental health provider; monitoring online behavior and communications (e.g., social media posts); and re-evaluating potential resources or support mechanisms to assist the employee in coping with stressors. Other strategies, particularly for high-risk cases, might include coordinating with law enforcement to issue a "stay away" order from the premises and notifying reception, front desk, or other personnel to contact security or law enforcement if the individual of concern is observed on premises following the separation.

These strategies are not exhaustive and not appropriate for all cases. BTAM teams should carefully consider these intervention methods in the full context of what is known about the individual and their environment. It can also be helpful to review the circumstances of the separation to assess organizational climate and potential interpersonal issues.

Terminating an employee does not eliminate the risk an employee poses. Separations can create other problems, such as exacerbating existing grievances and/or limiting the organization's ability to monitor the employee's behavior.

ZERO-TOLERANCE POLICIES

Zero-tolerance policies have historically been used in organizations as an assurance of safety for employees against risk of harm or violence. However, zero-tolerance policies have been shown, at times, to be overly punitive and inflexible to the unique circumstances and needs of individuals of concern. Zero-tolerance language also fails to account for early warning signs exemplified by concerning behaviors and communications prior to an incident occurring, and these policies can discourage some from reporting concerns. On a case-by-case basis, employers should consider whether using automatic punitive responses for employees of concern is the best approach for safety. BTAM teams should work with the employer to develop and implement a case management plan to effectively address the factors of concern for the employee, which may or may not involve punitive measures.

VOICES FROM THE FIELD

FROM A HUMAN RESOURCES PROFESSIONAL:

There are steps to take if someone has gone off track. As a manager, your responsibility is to coach the individual and help them … If that doesn't work, talk to them about what they are not doing right and what they need to fix. If someone is given every opportunity to get it right, and there is still no improvement, then it is time for a formal reprimand to prevent things from getting worse. Tell the employee what the next steps are, such as suspension, PIP, last chance agreement, or termination. Inform the employee of what they need to do for the entire time they are employed with you. There should be plenty of communication so that there are no surprises. You want to ensure people are not surprised that they're in trouble.

FROM A BTAM TEAM LEADER AT A HEALTHCARE AGENCY:

We provide assistance. That really helps in building trust and helps us with gathering information … Generally speaking, it's helpful to get people together so that they know what resources are available in the community. A lot of BTAM teams don't know about outside resources because of a lack of information sharing and partnering with others.

STRATEGIES FOR NON-EMPLOYEES

Organizations face unique challenges when trying to identify, assess, and manage individuals of concern that are not employed by the organization, including customers, clients, patients, visitors, and spouses or relatives of individuals connected to the workplace. The inconsistent or indirect contact between these individuals and the organization can make it difficult for the BTAM team to determine the extent of the risk the person might pose and may limit the management strategies and resources that can be provided. Organizations can use the following strategies to intervene and respond:

Determine the immediate security risks. Contact law enforcement for immediate safety concerns. In non-imminent situations, determine if law enforcement notification is appropriate.

Communicate with the individual of concern. Issue written or verbal warnings to individuals to articulate the organization's concerns, expectations for the individual's behavior, and what actions the organization will take if the individual continues to engage in a concerning manner.

Leverage community partners. Community partners with whom the organization has established a relationship (see Step 1) can be an asset during the BTAM process. Community partners may be leveraged by organizations so that individuals of concern may receive services, resources, or support. These community partners may also assist with searches of an individual's property, monitoring their behavior, or filing criminal charges.

Limit or restrict access. Limiting or revoking access to digital and physical spaces for problematic customers and visitors (e.g., restricting online accounts, issuing "no trespass" orders or barring notices) can help create a situation less prone to violence.

Alert employees. Issue alerts for employees to be on the lookout for an individual of concern and inform employees, including building security personnel, of what actions to take if they see the individual.

Enhance physical security measures. This can include stationing armed or unarmed security professionals at workplaces or using security cameras, metal detectors, or other security resources and devices.

Develop a strategy for continued monitoring. This can include allocating staff to search public court records and monitor open-source online activity and social media accounts.

IN PRACTICE: MANAGING RISK FOR NON-EMPLOYEES

ORGANIZATION 1: A multinational technology company frequently receives threats via their customer service sector. When a threat is received, the BTAM team runs queries to identify previous contacts with the customer and assesses whether this behavior is a trend and whether it is indicative of violent intent. From there, the team manages the customer by sending warnings, restricting access to the company's services, and identifying and notifying the company facility closest to the customer's location. If the situation escalates, the team contacts law enforcement.

ORGANIZATION 2: A nationwide healthcare network has a BTAM team that specializes in handling concerns related to their patients. When patients engage in problematic or concerning behaviors, a flag placed in the patient's digital record notifies staff. Staff also send letters to the patient's family to notify them of concerns. The organization has its own law enforcement personnel ready to respond to situations of imminent risk or crisis or when criminal activity is suspected or identified. The organization also employs mental health professionals, including counselors and social workers, who practice trauma-informed care and offer services to patients struggling with their mental health. The BTAM team can leverage partnerships with other personnel in their organization to assess and manage patients of concern.

VIOLENCE IN HEALTHCARE SETTINGS

Healthcare settings are disproportionately impacted by workplace violence compared to other settings. Data published in 2023 from the Occupational Safety and Health Administration (OSHA) suggested that healthcare workers were five times more likely to experience workplace violence than workers in other industries.[19] Rates of workplace violence in healthcare settings have also increased in recent years. In 2022, there were 24,590 cases of nonfatal injuries among healthcare and social assistance workers due to workplace violence, a 22.6% increase in the number of cases from 2019 data from the Bureau of Labor Statistics.[20] A majority of incidents in healthcare settings involve assaults perpetrated by patients or visitors against nurses and staff of emergency departments.

What strategies can help to prevent violence?

While many of the violence prevention strategies described in this publication can be useful for reducing the risk of violence in healthcare settings, healthcare organizations may also adopt other specific strategies to enhance the safety of patients, healthcare workers, and others. These strategies can include:

- Using ***behavioral agreements*** with patients who have exhibited aggression to outline appropriate behavioral conduct and consequences for violating the agreement.
- Providing regular training and roleplaying exercises to build staff skills in verbal and non-verbal ***de-escalation techniques*** to prevent escalating aggression.
- Using a ***trauma-informed care approach*** to help staff recognize and respond to signs of trauma in patients.
- Using ***electronic health record flags*** to alert staff when a patient has a history of aggression or violence.

STEP 7: PROMOTE A SAFE AND SUPPORTIVE ORGANIZATIONAL CLIMATE

A crucial component of workplace safety is developing an organizational culture of safety, respect, trust, and support. Positive organizational climates can reduce the risk of grievances and enhance bystander reporting when concerns are identified.

Organizational climate reflects how people perceive and describe their working environment, including employees' attitudes, feelings, and recurring patterns of behavior. Cultivating a positive climate of safety and support in an organization is important to ensure employees feel valued. Organizational climate also plays a vital role in preventing targeted workplace violence. Employees who feel respected and supported are less likely to view violence as an appropriate means of addressing their issues and may hold fewer and/or less intense grievances against their colleagues. Positive work climates can also have other important outcomes, including enhanced employee well-being, resilience, and productivity, as well as improved positive and supportive interactions with customers, clients, patients, and visitors.[21]

VOICES FROM THE FIELD

FROM A SECURITY DIRECTOR AT A MAJOR HEALTHCARE NETWORK:

For patients to be first, we need to have a healthy workforce to care for people. If employees are not healthy themselves, then they won't have a vested interest in our mission or the capacity to care for others. We tell employees not to wait for something to happen to say something, but to proactively engage in resources. If someone isn't feeling well due to finances, stress, depression, we have resources to offer our employees, including five free counseling sessions for them to use as they need.

STRATEGIES TO PROMOTE A SAFE CLIMATE

A variety of strategies can be instrumental to fostering a safe and supportive organizational environment.

Use safe hiring practices. Hiring decisions can be among the most impactful decisions made in an organizational setting, as the workforce cultivates their surrounding climate. Organizations should ensure that they employ safe hiring practices by measuring both an employee's aptitude (i.e., their anticipated ability to do their assigned work effectively) and their conduct (i.e., their ability to behave in ways that conform to the organization's rules, regulations, values, and norms). Organizations should be sure to follow all relevant federal, state, and local laws regarding hiring practices. When appropriate, organizations may consider supplementing a standard interview with background checks, reference checks, or a review of an applicant's digital footprint, such as a search engine lookup or social media review. When used appropriately, these strategies can be helpful in identifying patterns of hostile, concerning, inappropriate, criminal, or violent behaviors.

"BAN THE BOX" MOVEMENT

While organizations are encouraged to carefully consider an applicant's prior behaviors to make safe hiring decisions, it is important to avoid unfair hiring practices. Organizations sometimes use checkboxes to encourage applicants to self-disclose prior felony criminal convictions, then use the data to filter out applicants with felony convictions. Some civil rights movements, such as the "Ban the Box" campaign, have advocated for the removal of these checkboxes to promote fairness in hiring practices so that applicants with criminal histories can first be evaluated on their qualifications. Organizations must use caution to ensure that their hiring practices promote workplace safety while following federal, state, and local laws and simultaneously work to treat all applicants with fairness, dignity, and respect.

Respond fairly and effectively to problems. It is important for organizations to be proactive and to intervene early when concerns are easily managed, such as with minor disciplinary or performance issues. If unaddressed, these problems can escalate, causing further disruption or even violence. Disciplinary actions should not be used as punishment, but rather as corrective measures to educate employees about relevant issues with their performance and/or behavioral conduct and to inform them what actions are needed to get them back on the right track. Fairness, transparency, and consistency in the disciplinary process are important to help employees feel respected and to demonstrate the organization's commitment to a safe and positive work environment.

Address bullying and harassment at work. Bullying, harassment, and hostile or antagonistic behavior and attitudes can result in interpersonal conflicts and grievances, a fearful atmosphere, humiliation, and even perceptions of a hostile work environment. It is important to establish clear policies regarding workplace conduct and standards of behavior and to respond appropriately and proportionately to infractions. Disciplinary action may be appropriate in some instances, including reprimanding the aggressor, placing them on administrative leave, and/or terminating them from employment. Other strategies can also be effective in handling these matters, including alternative dispute resolution methods, conflict mediation, and transferring one employee to a different

work unit or facility. It may also be helpful to conduct climate assessments to gauge the overall organizational environment and identify factors that may have allowed these problematic behaviors to flourish.

Invest in employee resources. A key component to a positive organizational climate is ensuring employees feel heard, understood, and supported in the workplace. This can be achieved through offering resources to aid employees in their personal and professional lives, including EAPs, professional development opportunities, mental health support, employee resource groups, and peer support programs. These resources can be effective tools to enhance employees' coping skills, mental wellness, and sense of connection to their work, their colleagues, and their organization. Organizations can also collaborate with resources already available in their broader communities to develop a well-rounded menu of resources and opportunities.

Facilitate positive interactions. There are numerous characteristics of positive work environments, including clear and open communication, opportunities for growth and creativity, healthy work relationships, accountability, professionalism, respect, and the recognition of employee contributions and performance. These characteristics can be cultivated through practices, such as discussing office goals and values, practicing compassion and respect, offering praise for strong performance, checking in on employee well-being, facilitating social connections, and pursuing inclusivity and collaboration.

Cultivate a culture of safety. It is important for all employees to recognize safety as a priority and a community responsibility. Organizations should strive to foster a culture of safety in the workplace to ensure all employees understand their role in ensuring the workplace is safe from violence. Employees should be empowered to report the concerns they have in the workplace without fear of reprisal. All employees should understand the value of identifying, assessing, and managing concerns early, and all should recognize that the BTAM process is not intended to be punitive in nature.

VOICES FROM THE FIELD

FROM A HUMAN RESOURCES PROFESSIONAL:

You want to make sure you're listening to your staff, and that your staff feel heard. Employee engagement surveys are good. However, you need to take action on things that come up in surveys … If you don't, people will stop sharing their thoughts, and they will burn out. Make people feel integral to the organization. Help them understand what their role means for the strategic plan and organizational mission. This will take different shapes, depending upon the organization. But if you do it right, it's less likely someone will go off the deep end.

STEP 8: PROVIDE TRAINING FOR ALL EMPLOYEES

Training is essential for ensuring BTAM program success and workplace safety. Educating all employees on the BTAM program can promote trust, buy-in, and the reporting of concerns by staff. Organizations should consider the availability and accessibility, content, and frequency of training, and how to use continuous messaging to ensure employees are educated and empowered to contribute to violence prevention efforts.

Employee trust, buy-in, and reporting of concerns are critical elements for promoting BTAM program success. BTAM programs will not reach their full potential or will be underutilized if employees are not aware of the program, do not know what information to report or how to submit a report, and do not have trust in the process. Prior guidance for other settings, such as K–12 schools, emphasizes training and outreach as a best practice for enhancing bystander reporting. Training can also help support a positive workplace climate by fostering a shared understanding of BTAM and how programming supports employee safety through prevention.

Organizations should invest in training that provides all employees with the knowledge and resources necessary for violence prevention. Workforce training programs should consider training availability and accessibility, content, frequency, and continuous messaging.

AVAILABILITY AND ACCESSIBILITY

All employees should receive training on violence prevention efforts within their organization. Training sessions must be accessible to employees to support program success. Organizations should determine the appropriate medium for the training material (i.e., whether the training will be hosted in-person by a facilitator, through an online module, or some combination of these and/or other methods). Training modules should be sensitive to the employees' knowledge, experience, and time available. For instance, organizations may wish to consider the time employees typically spend on training modules, variance in primary speaking languages, and the audio and visual needs of the workforce.

CONTENT

BTAM training for employees should be included within the larger workplace training curriculum. Content specific to the BTAM process should be incorporated into workplace violence training to educate the general workforce about the process. When determining content, it is important to consider what employees need to know about the BTAM process and what their responsibility is in violence prevention. Training content might include:

- the definition of behavioral threat assessment and management;
- the guiding principles and goals of BTAM programming;
- an overview of how BTAM fits within the larger workplace violence prevention strategy;
- reference to relevant organizational BTAM policies;
- a general overview of the threat assessment and management process;
- information on the types of behaviors to report;
- how to report concerns;
- what to expect once a report has been submitted;
- expectations about confidentiality; and
- an overview of employee protections, including policies against retaliation for reporting.

FREQUENCY

All employees should be regularly trained on workplace violence prevention. Organizations should deliver workplace violence prevention training during new employee orientation and establish cycles for refresher training. BTAM teams should determine the frequency of these refresher trainings based upon organization size, turnover rate, and available resources, and they should account for how BTAM education modules fit into the wider employee training schedule.

IN PRACTICE: TRAINING FOR ALL EMPLOYEES

A healthcare organization has shifted from a broad all-service awareness training model to a more tailored approach, utilizing small group sessions, personalized discussions, and team meetings to connect with personnel. The organization has also been intentional with the frequency of electronic communication, steering clear of oversaturating inboxes with messaging, and instead using a combination of electronic communication and other types of messaging at the physical job site. This includes flyers, pamphlets, and posters in bathroom stalls. The organization has found these more intentional forms of raising awareness on workplace violence prevention to be more effective than the traditional all-service awareness training approach.

CONTINUOUS MESSAGING

Organizations should establish general messaging efforts and initiatives specific to the BTAM process. This can include infographic posters that educate employees on how to report concerning behaviors, regular reminders on workplace safety efforts in the organization, and information on available resources for support. Continuous messaging supports workplace violence prevention education between training cycles.

VOICES FROM THE FIELD

FROM A SECURITY DIRECTOR FOR A HEALTHCARE SYSTEM:

The overall goal is to reduce fear through education. Enhancing situational awareness and training people on how to respond is critical.

FROM A BTAM TEAM AT A GLOBAL ORGANIZATION:

We did very successful awareness sessions where we got in front of specific teams—human resources, legal, and others—and we identified concerns we're looking for. We taught them how we don't want to wait for someone to punch someone else. Instead, if you start seeing behaviors, especially a cluster of behaviors, you take action then. We started these trainings four or five years ago, and we still get contacted about them. These were really successful with middle management especially, who would then start to advocate on our behalf.

FROM A SECURITY DIRECTOR AT A MAJOR ENTERTAINMENT COMPANY:

We have found micro-learnings to be one of the most helpful tools in educating the masses at our organization. We have been able to distill content into short videos that we make available online. Each video ranges in length from 9-12 minutes. This is helpful in educating our employees on really important topics, including workplace violence prevention, in a timeframe that is conducive to other tasks they are managing. These micro-learnings also help us reach employees across multiple worksites and time zones.

CONCLUSION

The U.S. Secret Service has long held that prevention is the best form of protection. For over 25 years, NTAC's research examining incidents of targeted violence has demonstrated that future tragedies are preventable if communities are equipped with the training and resources necessary to identify individuals of concern, assess their risk of violence, and intervene appropriately.

This publication offers both research and guidance intended to help organizations and their partners recognize concerning behaviors and intervene before violence can occur. By following the steps in this operational guidance, organizations and their community safety partners can adopt the pioneering principles of the Secret Service's model for behavioral threat assessment and management and move toward a structured approach to preventing targeted workplace violence.

NTAC recognizes that many of the steps in this guidance depend upon organizations and communities having important resources available to assist throughout the BTAM process. As such, the steps within this guide are intended to be scalable to organizations of varying sizes and resources, all with the shared mission of preventing targeted workplace violence within their communities. Everyone has a role to play in keeping communities safe, and the Secret Service stands ready to support our public safety partners in this vital mission.

APPENDICES: DATA TABLE 1

INCIDENT DATA	All Attacks	Current or Former Employees	Customers, Clients, Patients, and Visitors	Romantic Partners and Relatives
	***n* = 50 / 29%**	***n* = 22 / 13%**	***n* = 19 / 11%**	***n* = 9 / 5%**
Weapons*				
Firearms	86%	95%	68%	100%
Bladed Weapons	14%	0%	37%	0%
Vehicles	2%	5%	0%	0%
Explosive	2%	5%	0%	0%
Incendiary	2%	5%	0%	0%
Other	2%	5%	0%	0%
Location Types*				
Businesses	**86%**	**95%**	**74%**	**89%**
Restaurants/Bars	20%	5%	37%	22%
Retail	6%	9%	0%	11%
Services	22%	23%	21%	22%
Manufacturing/Distribution	20%	45%	0%	0%
Healthcare	14%	9%	16%	22%
Government/Military	6%	9%	0%	11%
Government	*4%*	*5%*	*0%*	*11%*
Military	*2%*	*5%*	*0%*	*0%*
Residential Community	**4%**	**0%**	**11%**	**0%**
Open Space	**8%**	**9%**	**5%**	**11%**
School	**2%**	**0%**	**0%**	**11%**
Non-profit Services	**4%**	**0%**	**11%**	**0%**
Motives*				
Grievance	88%	95%	79%	89%
Personal	*38%*	*18%*	*68%*	*22%*
Workplace	*36%*	*77%*	*5%*	*0%*
Domestic	*22%*	*14%*	*5%*	*78%*
Psychotic Symptoms	12%	23%	0%	11%
Ideology	2%	0%	5%	0%
Fame or Notoriety	2%	5%	0%	0%
Desire to kill	4%	5%	5%	0%
Other	2%	5%	0%	0%
Undetermined	6%	0%	16%	0%
Total Casualties (Injuries + Deaths)	**247 (4.94 avg)**	**125 (5.68 avg)**	**92 (4.84 avg)**	**30 (3.33 avg)**
Injured	128 (2.56 avg)	63 (2.86 avg)	57 (3.00 avg)	8 (0.89 avg)
Killed	119 (2.38 avg)	62 (2.82 avg)	35 (1.84 avg)	22 (2.44 avg)
Resolution				
Attackers stopped on their own, then...	**76%**	**77%**	**68%**	**88%**
Arrested at/away from scene	30%	22%	37%	35%
Committed suicide	46%	54%	31%	54%
Law enforcement intervened, then...	**18%**	**23%**	**15%**	**12%**
Arrested at/away from scene	4%	0%	10%	0%
Killed by law enforcement	14%	23%	5%	12%
Bystanders intervened, then...	**4%**	**0%**	**11%**	**0%**
Arrested at/away from scene	2%	0%	6%	0%
Other	2%	0%	6%	0%
Weapon rendered inoperable, then...	**2%**	**0%**	**5%**	**0%**
Arrested at/away from scene	2%	0%	5%	0%

*Indicates multiple responses.

APPENDICES: DATA TABLE 2

ATTACKER DATA	All Attackers	Current or Former Employees	Customers, Clients, Patients, and Visitors	Romantic Partners and Relatives
	n = 51 / 28%	*n* = 22 / 12%	*n* = 20 / 11%	*n* = 9 / 5%
Gender				
Male	96%	95%	95%	100%
Female	2%	0%	5%	0%
Other	2%	5%	0%	0%
Age Range (average)	**22-66 (41.0 avg)**	**22-64 (40.1 avg)**	**23-66 (41.1 avg)**	**27-58 (42.9 avg)**
Race/Ethnicity				
White (non-Hispanic/ethnicity unknown)	41%	32%	55%	33%
Black/African American	29%	50%	10%	22%
Hispanic/Latino	14%	9%	20%	11%
Asian	12%	9%	5%	33%
Undetermined	4%	0%	10%	0%
Arrests/Charges	**65%**	**64%**	**70%**	**56%**
Domestic Violence	18%	9%	20%	33%
Sex Crimes	8%	9%	10%	0%
Other Violent Crimes	31%	27%	35%	33%
Non-Violent Crimes	57%	55%	65%	44%
History of Domestic Violence*	**53%**	**41%**	**55%**	**78%**
Mental Health Symptoms	**59%**	**64%**	**55%**	**56%**
Known Treatment/Diagnosis	39%	36%	45%	33%
Psychosis	29%	41%	20%	22%
Paranoia	22%	41%	5%	11%
Delusions	12%	23%	0%	11%
Hallucinations	10%	18%	0%	11%
Depression	29%	32%	20%	44%
Suicidal Ideations/Attempts	18%	14%	15%	33%
Stressors (within 5 years of attack)	**92%**	**91%**	**95%**	**89%**
Triggering Event	43%	32%	60%	33%
Financial Instability	55%	59%	55%	44%
Personal Stressors	47%	50%	45%	44%
Romantic Stressors	39%	26%	25%	78%
Employment Stressors	45%	73%	15%	44%
Concerning Communications	**75%**	**77%**	**65%**	**89%**
History of Making Threats	47%	41%	40%	78%
Threat Specific to the Target	31%	32%	25%	56%
Indicating Imminence of Attack	8%	5%	5%	11%
Elicited Concern	**78%**	**82%**	**75%**	**78%**
Elicited Concern at Work	24%	41%	10%	11%
Elicited Concern for Safety	61%	41%	75%	78%
Bullying/Harassment				
Victim of	18%	36%	5%	0%
Perpetrator of	47%	41%	40%	78%
Inappropriate Interest in Violence or Weapons	**10%**	**9%**	**10%**	**11%**
Behavior Change	**41%**	**55%**	**25%**	**44%**

*Indicates at least one incident of domestic violence which may or may not have resulted in an arrest or criminal charge.

[1] National Threat Assessment Center. (2023). *Mass Attacks in Public Spaces: 2016 – 2020*. U.S. Secret Service, Department of Homeland Security. www.secretservice.gov/ntac.

[2] Society for Human Resources Management. (n.d.). "It's critical to distinguish between performance and conduct issues." www.shrm.org.

[3] Cybersecurity and Infrastructure Security Agency. (2020). *Insider Threat Mitigation Guide*. Department of Homeland Security. www.cisa.gov.

[4] Bureau of Labor Statistics. (2026). "National census of fatal occupational injuries, 2023–2024." Department of Labor. www.bls.gov.

[5] Bureau of Labor Statistics. (2026). "Nonfatal cases involving days away from work, 2023–2024." Department of Labor. www.bls.gov.

[6] Office of the Assistant Secretary for Administration & Management. (n.d.). "DOL workplace violence program." Department of Labor. www.dol.gov.

[7] California Department of Industrial Relations. (2024, June). "Workplace violence prevention in general industry (non-health care settings) – Information for employers." Division of Occupational Safety & Health, State of California. www.dir.ca.gov.

[8] Centers for Disease Control and Prevention. (2026, August 19). "About intimate partner violence." Department of Health and Human Services. www.cdc.gov.

[9] Centers for Disease Control and Prevention. (2003, March). *Costs of Intimate Partner Violence Against Women in the United States*. Department of Health and Human Services. www.cdc.gov.

[10] Federal Bureau of Investigation. (n.d.). *Workplace Violence: Issues in Response*. Department of Justice. www.fbi.gov.

[11] ASIS International. (2020). *Workplace Violence and Active Assailant – Prevention, Intervention, and Response*. www.asisonline.org.

[12] Cybersecurity and Infrastructure Security Agency & U.S. Secret Service. (2023). *Improving School Safety Through Bystander Reporting: A Toolkit for Strengthening K–12 Reporting Programs*. Department of Homeland Security. www.secretservice.gov/ntac.

[13] Cybersecurity and Infrastructure Security Agency. (2020). *Insider Threat Mitigation Guide*. Department of Homeland Security. www.cisa.gov.

[14] Security Executive Council. (2025). *Executive Targeting Report: Analysis of Attacks on Corporate Executives from 2003–2025*. www.securityexecutivecouncil.com.

[15] Allied Universal. (2026). *World Security Report 2026*. www.worldsecurityreport.com.

[16] ASIS International. (2025). *The Executive Threat Environment: Benchmarking Research on Risk-Based Approaches to Executive Protection*. www.asisonline.org.

ENDNOTES

[17] National Threat Assessment Center. (2024). *Behavioral Threat Assessment Units: A Guide for State and Local Law Enforcement to Prevent Targeted Violence*. U.S. Secret Service, Department of Homeland Security. www.secretservice.gov/ntac.

[18] Attridge, M. (2022). Profile of small employers in the United States and the importance of employee assistance programs during the COVID-19 pandemic. *American Journal of Health Promotion, 36*(7). www.pmc.ncbi.nlm.nih.gov.

[19] Occupational Safety and Health Administration. (2023). "Healthcare: Workplace violence." Department of Labor. www.osha.gov.

[20] Bureau of Labor Statistics. (2023). "Nonfatal cases involving days away from work, 2022." Department of Labor. www.bls.gov.

[21] Cybersecurity and Infrastructure Security Agency. (2023). "Preventing workplace violence: Security best practices." Department of Homeland Security. www.cisa.gov.

SECRET
SERVICE

U.S. DEPARTMENT OF HOMELAND SECURITY

UNITED STATES SECRET SERVICE

NATIONAL THREAT ASSESSMENT CENTER