From protective intelligence to threat assessment: Strategies critical to preventing targeted violence and the active shooter

Matthew Doherty

Received (in revised form) 19th February, 2016

Senior Vice President, Hillard Heintze, 30 S. Wacker Dr., Suite 1400, Chicago, IL 60606, USA.
Tel: +1 312-229-9826; e-mail: Matthew.Doherty@hillardheintze.com

Matthew Doherty

__Matthew Doherty__ is SVP in Hillard Heintze's Federal Practice, with over 24 years' experience leading law enforcement and intelligence programmes and investigations in the prevention of violence by developing and enhancing methodologies with national security priorities. He is widely recognised as among the most experienced senior experts in assessing an individual's potential for danger and preventing targeted violence against national leaders, national critical infrastructure, major events and corporate workplaces. As a thought leader in targeted violence, workplace violence prevention and active shooter planning, he leads Hillard Heintze's Security Risk Management, delivering the full spectrum of the firm's investigations, security risk management and law enforcement advisory services to clients in the Washington, DC area. He oversees large-scale, private sector security engagements. Earlier in his career, he served as the Special Agent in Charge of the US Secret Service National Threat Assessment Center. In this capacity, he managed training on threat assessment and targeted violence prevention for federal, state and local law enforcement personnel. He created the first information-sharing database (TAVISS) for the prevention of violence against protected officials. He is an advisor to the Department of Homeland Security, Science and Technology Directorate and the DHS Operating Elements in addressing important homeland security issues. He also serves on the US Marshal Service Judicial Threats Center for preventing violence against judges. He is a law enforcement advisor and trustee award winner with DHS's Homeland Security Studies and Analysis Institute. He is Senior Fellow at the George Washington University Center for Cyber & Homeland Security.

Abstract

Acts of targeted violence — including active shooter incidents — are typically over within 15 minutes, often before the first law enforcement personnel can respond to the scene. More than a third of active shooter incidents in the USA, for example, last less than five minutes. While this stark fact is often used, with unimpeachable validity, as the cornerstone of employee security awareness training and the need for each employee to make a quick decision on whether to run, hide or fight, it also underscores the importance of another critical priority: prevention. This paper focuses on several of the most effective strategies and tactics — increasingly used across the USA, but applicable all over the world — in preventing an act of targeted violence or active shooter event. It starts *with a brief discussion of the common roadblocks to prevention within enterprises today as well as the warning signs that can reveal an individual's path toward an act of violence. Next, it defines targeted violence and summarises patterns that research has helped uncover with respect to attackers' backgrounds, motives and target selection. This paper also outlines the crucial role played by protective intelligence and threat assessment protocols and provides several case studies to illustrate key concepts in real-world applications. Finally, this discussion points to several emerging trends in the USA and Europe, among other regions — such as radicalisation within the workforce — that are likely to continue to mature in 2016 and the years ahead.*

Keywords: protective intelligence, threat assessment, workplace violence, targeted violence, active shooter, security

INTRODUCTION

Sandy Hook's elementary school. Aurora's movie house. Paris's Bataclan Theatre. Nairobi's Westgate Shopping Mall. Today, the names of these places are recognised across the world for the wrong reasons. They are now headlines seared into our collective conscience like the names of early battles in a war that corporate executives, senior administrators and school principals have not necessarily been trained to address.

The harsh reality is that — in one form or another — targeted violence, including but not limited to terror, is now happening with rising frequency in workplaces, public locations and schools on a regular basis. In the US, on average, 1.7 million people annually are victims of violent crime while working — including an average of 700 homicides per year.[1] What even many directors of public safety and security don't yet realise is how wide a body of knowledge — key principles, best practices and cost-effective counter-strategies — is now available to help minimise the risks of such a devastating event. In other words, we actually know how to counter this threat.

The challenge is that many employers and sometimes even their experts in security, business continuity and emergency preparedness aren't always aware of the full spectrum of these countermeasures. As a result, they are not sufficiently integrating the crucial steps necessary to protect their leaders and employees as well as their facilities and the continuity of their operations.

THE NEED TO FOCUS ON PREVENTION

From our perspective, it's not that organisations aren't taking action. They are. In one way or another, many are trying hard to recognise the risk and place the right resources behind addressing it. But some efforts are missing the mark.

Why? More than a few organisations are overly focused on making sure the right steps are taken *after* an event has occurred. They're focused on managing a crisis — responding quickly and in force. They're focused on training employees to silence their phones the moment that shots are first fired and to be prepared to use their three best life-saving options: run, hide or fight. They're focused on containing the threat and on quickly communicating the danger to personnel within the facility without the delays — like those that resulted in so many deaths at Virginia Tech.

All of these steps are important. But they're not enough. What companies, public agencies and academic institutions also need to do is minimise the likelihood that these acts of targeted violence will ever occur in the first place. They need to ensure that their strategy and plan is based not just on response and recovery but also on prevention and the mitigation of risk well before an event occurs.

COMMON ROADBLOCKS TO PREVENTION

Multiple factors impede targeted violence prevention. These include a lack of awareness about the knowable indicators of a potential attack; poor understanding of risk and mitigation measures; limited cross-functional collaboration and information sharing; and an absence of an overall strategy to address targeted violence prevention.

WARNING SIGNS: TWO EXAMPLES IN THE USA

There are almost always signs — if you know what to look for. Take the Navy Yard shooting in Washington DC, for example, on 14 September 2013. The shooter was cited at least eight times for misconduct for offences as minor as a traffic ticket and showing up late for work, but also as serious as insubordination and disorderly conduct, according to a Navy official, who spoke on condition of anonymity to discuss the gunman's personnel record. In fact, the company that employed the Washington Navy Yard shooter pulled his access to classified material for two days in August when mental health problems became evident, but restored it quickly and never told Navy officials about the withdrawal.

Consider a more recent example: the fatal shootings of Adam Ward and Alison Parker on 26 August 2015. As the *New York Times* reported,[2] the shooter, Vester Lee Flanagan II had a 'turbulent tenure' at WDBJ, the television station in Roanoke, Virginia, where his victims worked and he had been formerly employed. In 2012, he had 'a heated confrontation' with a reporter. Less than a month later he clashed with a photographer and within a week, he confronted one of the station's photographers. Documents revealed that these and other actions led to Flanagan's referral to the TV station's Employee Assistance Programme. His behaviour, he was told, 'resulted in one or more of his co-workers feeling threatened or uncomfortable'.

As with other acts of targeted violence, each of the clues by themselves may not mean much, but when viewed collectively by an outside expert or internal threat management team, they can begin to suggest a pattern. That process of analysis starts with a clear definition and the opportunity for early intervention and risk mitigation.

TARGETED VIOLENCE: A BRIEF DEFINITION

Targeted violence is any incident of violence in which a known or knowable attacker selects a particular target prior to their violent attack. Countering the risks related to targeted violence and the active shooter first requires the following:

- Dispelling common myths and false beliefs about attackers and their motives and tactics.
- Understanding key elements at the core of the pre-attack process.
- Learning how to leverage countermeasures such as behavioral threat assessment and protective intelligence.

MYTHS AND MISCONCEPTIONS ABOUT ATTACKERS

Some of the most actionable information on targeted violence is quite new. Twenty-five years ago, the US Secret Service was still in the early stages of developing insight into the motivations and behaviours of people capable of unleashing this type of violence on others. In the late 1980s, for example, several serious Secret Services cases challenged the agency's traditional beliefs about assassins and their behaviour. These beliefs were based on assumptions that a person posing a threat: (1) had a single direction of interest; (2) would make an explicit threat; (3) held hostility toward his or her target; and (4) would bring himself or herself to the attention of the Secret Service.[3] In each and every one of these serious cases, the Secret Service did not become aware of the subject until after he or she had appeared on site with a weapon. This realisation was, in part, a key driver behind the Secret Service's decision to launch a landmark inquiry into the mind of an attacker.

THE ATTACKER'S MINDSET: SEMINAL RESEARCH

In 1992, the US Secret Service (USSS) and National Institute of Justice (NIJ) launched the Exceptional Case Study Project. This was a five-year study that examined the thinking and behaviour of 83 individuals who have attacked or approached to attack prominent public officials or figures in the USA from 1949 to 1996. Twenty-four of the 83 attackers were interviewed. The study determined that out of the 74 attacks studied, six were carried out by 16 individuals who were members of a group, and 68 attacks were carried out by 67 individuals acting alone. The study's outcomes still guide our knowledge of targeted violence and its prevention today.

(1) **Myths and facts** — One early misconception was that attackers fit a distinct profile. The study suggested, however, that they do not align neatly with a descriptive or demographic profile. Another myth was that attackers are often mentally ill and may be too irrational to carry out a sophisticated attack when in fact they are extremely well organised. A third is that attackers make direct threats. The study indicated, however, that people who *pose* an actual threat most often do not actually *make* one.

(2) **Core facets of the pre-attack process** — The study revealed that the pre-attack process involves an understandable and often discernible process of thinking and behaviour. It stems from an interaction among the potential attacker, past stressful events, a current situation and the target. The study also strongly suggested that a potential attacker's behaviour is vital to identifying his or her intentions; the attacker's thinking, planning and logistical preparations have to be detected and interrupted.

(3) **Common backgrounds of attackers** — Many feel despair, suffer from depression or have suicidal thoughts. Some have a history of harassing or stalking, or have suffered a major loss or change in life. Despite what some may believe, few have been arrested for violent crimes. Attackers also tend to engage in attack-related behaviours including: (a) interest or obsession with violence; (b) development of attack plan; (c) approach or visit site of attack; (d) attempted assault or actual attack; (e) attempt to penetrate security; and (f) approach or visit site with weapon.

(4) **Motives and target selection** — Some attackers want to achieve fame and notoriety. Others are attempting law enforcement-assisted suicide or to bring national attention to a perceived problem.

THREAT ASSESSMENT: THE BACKBONE OF PREVENTION

In the years since the joint USSS and NIJ study, the field of behavioral threat assessment has expanded beyond its initial focus on preventing individuals bent on assassinating a political leader to stopping those who may have the interest, motive, intention and capability of committing an act of targeted violence in, for example, the workplace, a public space or an academic environment.

Today threat assessment is a highly specialised area of inquiry that does not fit neatly within the purview of law enforcement, psychology or even protective intelligence. Instead it spans and requires a careful choreography of them all.

In short, the speciality involves three key processes: (1) identification of individuals who have the idea of or intent to attack; (2) assessment of the individual by gathering information from multiple sources in order to determine whether they post a risk; and (3) management of the individual's case.

Information gathered on the subject includes his or her mental history, current life situation, behavioral history, motivation, attack-related behaviour, facilitating and mitigating factors, criminal history, media records, organisation interest and affiliation, specialised training, and ownership or ability to acquire weapons. Methods of acquiring this information include background examination; interviews with family and key contacts; review and analysis, if relevant, by clinical psychologist; liaison and facilitation with law enforcement and protective intelligence authorities; and counter-threat recommendations and assistance.

Using this information, experts evaluate the subject across several critical outcome-signalling dimensions to assess his or her potential for committing an act of targeted violence. Specifically, these dimensions include, for example: (1) organisational ability; (2) fixation; (3) focus; (4) action; and (5) time imperative.

A FOCUSED SET OF QUESTIONS

What are the questions threat assessment experts seek answers to? Here is a representative sampling.

(1) What motivated the subject to make the statement or take the action which caused him or her to come to our attention?

(2) What has the subject communicated to anyone concerning his or her intentions?

(3) Has the subject shown inappropriate interest in assassins, weapons, militant ideas or mass murders?

(4) Is there evidence that the subject has engaged in attack-related behaviour targeting our protectee(s)?

(5) Does the subject have a history of mental illness involving command hallucinations, delusional ideas, feelings of persecution, etc.?

(6) Does the subject have the ability to plan and execute a violent action against one of our protectees?

(7) Is there evidence that the subject is experiencing desperation and/or despair?

(8) Is what the subject says consistent with his or her actions?

(9) Is there concern among those who know the subject that he or she might take action based on inappropriate ideas?

(10) Are there factors in the subject's life or environment which might increase or decrease the likelihood of the subject attempting to attack a protectee?

CASE IN POINT: MANAGING A STALKER INCIDENT

Predicting an individual's dangerousness is one thing. Doing so in time to prevent harm to others requires real-time — or near real-time — access to information and an informed ability to interpret this information, ideally in the context of an extensive understanding of the subject's background, history and life circumstances. Here's an illustration of some of the principles applied to a particular real-world scenario. This company is a diversified real estate investment trust with a multi-floor office in a major city. Its Human Resources (HR) department received a complaint from an anonymous caller that one of its receptionists was slandering the management team. The company prepared to take action but it quickly learned that the caller was an individual known to their employee who had been stalking her for over a year. Within a week or so, their outreach to local law enforcement resulted in a visit to the office by a police officer and an initial flurry of incident reports and administrative filings. But thereafter, progress in the case quickly stalled.

Over the next ten days, an integrated team of protective intelligence experts, behavioral threat assessment specialists and retired law enforcement executives worked closely with the company, its security and legal departments, mental health professionals and the employee herself — as well as appropriate local, state and federal authorities — to uncover information about the caller and ensure the safety of the receptionist. Every case is different — and the most appropriate courses of action depend on factors such as the urgency of the threat-related circumstances, case history, information known and available about the alleged stalker, and to what extent the parties involved seek protection, intervention and prosecution, among many other tactics, strategies and outcomes.

In this particular case, the expert team's first order of business was obtaining a photo of the subject for dissemination to employees and facility staff. Hillard Heintze's experts also contacted former colleagues at a major federal agency, determined their primary points of contact with local law enforcement and mounted a multi-jurisdictional team of both internal and external experts that began responding quickly. Next, the firm conducted an investigation of the alleged stalker, analysed his 'dangerousness' and potential to inflict harm, and advised the company and employee on key findings, options, recommendations and next steps.

EIGHT CRITICAL SEATS TO FILL ON THE THREAT ASSESSMENT TEAM

In the case outlined above, the organisation was large enough to have supported the creation of a threat assessment team, which could have played a leadership role in addressing this threat. Many disciplines must be represented. A multidisciplinary team with members from many facets of the workplace and community is enriched by diverse perspectives, as well as access to many more sources of information.

But every business and key facility has different requirements. Some depend on factors such as the industry, business model, size of location, number of employees, type of skill sets on premises, history of labour relations, and economic conditions at both the national and the local level. Other requirements depend on a host of hard-to-measure influences such as office or shop-floor culture, attitudes toward management, and employee concerns related to privacy, communications and personal hardships at work or at home.

At minimum, membership of the threat assessment team should include representatives from the following:

(1) Security Department — Security personnel play a key role at many phases.
(2) Human Resources Department — HR representatives are especially

helpful if an employee displays behaviours of concern.

(3) Legal Services — Legal relations representation is critical to ensuring proper definition of all legal issues during a case management. In some circumstances, legal services staff can lead efforts to obtain protective orders or engage in other legal procedures related to the team's activities.

(4) Supervisors — These individuals are often the 'first line of defence' in detecting and monitoring 'behaviours of concern' within a workforce.

(5) Local Mental Health Liaison — If not included as regular members of the team, these professionals should be notified of its existence and included as ad hoc members when needed for information sharing.

(6) Labour Unions — Both management and union leaders have a mutual responsibility to ensure a safe workplace environment for employees. Unions can play a key role in preventing acts of workplace violence.

(7) Local Law Enforcement — A memorandum of agreement should be developed with the police department so its representatives are able to fully participate as members of the threat assessment team when necessary.

(8) External Threat Assessment Experts — These individuals can be useful in supporting the team's adoption of best practices and gaining perspectives on how other organisations have handled comparable issues and challenges. One such expert who can be invaluable is a clinical psychologist with experience in threat assessment.

CASE IN POINT: THE FACEBOOK THREAT

In this second real-world example, an employee in a branch office of a major national provider of outsourced business solutions posted threatening statements about company personnel on his Facebook wall, along with several pictures of himself posing with weapons.

Within hours, threat assessment experts were on site, reviewing internal human resources files and reports and conducting a battery of discreet interviews with the subject's known associates and others with a direct perspective on the events occurring in his life. The team tapped its national network of contacts to facilitate a meeting with the chief of the local police department, who assigned one of his top investigators as a liaison to the team. Other analysts began an immediate background investigation of the subject and started assessing emerging information — in real time — using the methodology outlined earlier in this paper.

With this expert support, the company identified and considered a range of potential countermeasures, selected one with a high probability of success, and implemented it. One employee, who had been a target of the subject's anger, was temporarily reassigned to offices in another state. No act of targeted violence occurred. Even after the individual who posted the statements was terminated through a carefully orchestrated series of steps, the company and its external advisors continued to manage the threat on an ongoing basis — in part, by supporting the individual's access to mental health treatment and the opportunity to move his life forward in a healthier and more positive way.

ACTIVE SHOOTER PREVENTION: A GROWING PRIORITY

Let's focus the discussion now on one type of targeted violence: an active shooter incident. An active shooter is an individual who is actively engaged in killing or attempting to kill people in a confined and populated area. Based on a recent study, the average attack lasts approximately 12 minutes, and 37 per cent lasted less than five minutes.[4] There is little time to react.

An active shooter plan should consist of four key components: Prevent and Mitigate, Prepare, Respond, and Recover. The prevention and mitigation phase includes workplace violence prevention measures such as screening employees before and during employment, establishing an employee assistance programme, conducting threat assessments, holding active shooter training and assembling an active shooter committee.

Organisations and their departments, such as Security or Human Resources, can take a leadership role in the pre-planning and training process by working with first responders, including police, fire and medical, as well as all departments and key stakeholders, including management and leadership.

During the response phase, individuals should follow the US Department of Homeland Security's Run, Hide, Fight guidelines. This should also include the implementation of internal and external emergency management plans, coordinating incident command posts and establishing a media relations centre.

Following an incident, as normal operations — both internal and external — are restored, debriefings must be held, as well as post-incident press conferences and multidisciplinary debriefings. An after-action report should also be conducted.

RADICALISATION WITHIN THE WORKPLACE: AN EMERGING PRIORITY FOR WESTERN EMPLOYERS

As the techniques and tactics used to prevent targeted violence continue to evolve, new challenges will materialise in 2016 and the years ahead for companies with corporate facilities in the United States and other Western nations. Among the most prominent emerging risks this year is what many experts will increasingly refer to as 'radicalisation in the workplace'. One effective definition of this phenomenon — which carries many implications for targeted violence prevention strategies — is a process by which an individual or group comes to adopt increasingly extreme political, social or religious ideals and aspirations that reject or undermine (1) the status quo or (2) expressions of freedom of choice. The spectrum of potential behaviour that could be 'radicalised' ranges from domestic issues such as — in the USA, for example — gun rights, abortion, racism, animal rights and LGBT issues to international issues such as ultra right or left-wing activism and religious extremism.

While a detailed discussion of this trend and its relationship to targeted violence prevention stands outside the scope of this paper, this will likely prove itself to be, in the words of Alan Lipman, Founder and Executive Director of the Center for the Study of Violence in Washington, DC: 'a change in the nature of mass shootings in the US. No longer are they solely defined by a single, isolated aggrieved shooter but a shooter or shooters embedded in, justified by and potentially supported by an ongoing ideological framework.'

CONCLUSION: TARGETED VIOLENCE PREVENTION IS NOT BEST LEFT TO LAW ENFORCEMENT

Whichever strategies and countermeasures an entity elects to pursue to manage the risks of targeted violence, it is important to remember that prevention starts internally — within the organisation. Although actual violence is still rare in most organisations, other disturbing, threatening and troubling behaviours in the workplace affect more than just the persons directly involved.

An established workplace violence prevention programme within the organisation creates the opportunity for early intervention and risk mitigation. A proactive approach to prevent workplace violence creates security awareness and a sense of responsibility for all employees to report concerning behaviours. An organisation's commitment to maintaining a safe workplace creates higher employee morale, better productivity and uninterrupted business operations.

Traditional law enforcement practices and personnel focus primarily on procedures after a crime has taken place: investigating the event, seizing evidence, arresting suspects and prosecuting the accused. In fact, unless law enforcement officials have received specific training on violence prevention and threat assessment, they are not likely to take advantage of information reported to them in an effective manner. And in a worst-case scenario, they may be unable to respond in any meaningful way at all.

By the time an event has occurred, the organisation has almost certainly missed at least several opportunities — to prevent it or at least mitigate the most serious impacts and consequences. Thinking ahead will save lives.

Acknowledgement

The author would like to acknowledge Todd Kreisher as a contributing subject matter expert on this paper.

References

(1) Source: Centers for Disease Control and Prevention, Bureau of Labor Statistics' Census of Fatal Occupational Injuries (CFOI).

(2) Shear, Michael et al. 'Ex-broadcaster kills 2 on air in Virginia shooting; takes own life', *New York Times*, 26 August 2015.

(3) Fein, R. A. and Vossekuil, B. (1999) Assassination in the United States: An operational study of recent assassins, attackers, and near-lethal approachers. *Journal of Forensic Sciences*, 50, 321–33.

(4) US Department of Homeland Security. Planning and Response to an Active Shooter: An Interagency Security Committee Policy and Best Practices Guide. November 2015.