VOLUME 4, ISSUE 1 | JULY 2026

Volume 4, Issue 1

Published by the International Protective Security Board

July 2026

The CLOSE PROTECTION & SECURITY JOURNAL

Protection begins with understanding.

The International Protective Security Board is an independent, volunteer organization devoted to promoting the protection industry's interests and professionalization.

The CLOSE PROTECTION & SECURITY JOURNAL

Contents

Letter from the Editors

Every profession evolves. Sometimes the change is gradual enough that no one notices until they look back and realize the work has fundamentally changed. We believe protective security is at one of those moments. For decades, close protection has been understood primarily as a physical discipline. The image most people have is still the same, which is of a protector standing beside a principal, scanning the crowd, driving the motorcade, or responding decisively when something goes wrong. Those capabilities remain essential. They always will, but they no longer define the profession.

Ever more, the threats we confront do not begin with an attack. They begin with a series of small developments that, taken individually, appear unremarkable: a grievance expressed online, changes in behavior, an overlooked legal issue, a medical condition, an information leak, a piece of surveillance that goes unnoticed, or a pattern hidden within seemingly unrelated data. By the time violence occurs, the opportunity to prevent it has often already passed. That reality changes what it means to be a protection professional. The question on security moves from "*Can we respond effectively?"* to "*Can we recognize the risk before intervention becomes necessary?"* Answering that question requires a different way of thinking. It requires understanding.

That idea has become the guiding philosophy of this journal: Protection begins with understanding. We chose those words carefully. Protection has always depended on knowledge, but today's operating environment demands something broader than tactical expertise alone. The modern protector must understand people as much as places, systems as much as procedures, and risk as much as response. Law matters. Psychology matters. Medicine matters. Intelligence matters. Technology matters. None of these disciplines sit neatly outside protective security anymore. They have become part of it.

Perhaps that is the most important development occurring within our profession. Protective security is becoming more analytical. We are moving beyond the idea that our primary value remains in reacting to crises. Instead, our value progressively lies in helping prevent them. That is a significant shift.

It also reflects the continuing maturation of the profession itself. Protective security is no longer built solely on experience passed from one practitioner to another. It is becoming supported by research, evidence, and interdisciplinary thinking. Questions once answered by instinct alone are now being examined through behavioral science, intelligence analysis, legal scholarship, executive medicine, investigative methodology, and emerging technologies. Far from diminishing experience, this body of knowledge strengthens it by giving practitioners better ways to understand increasingly complex problems.

That evolution is reflected throughout this issue. The subjects vary considerably, yet they all point toward the same conclusion. Whether the discussion concerns legal authorities, behavioral threat assessment, technical surveillance countermeasures, executive health, investigative analytics, or protective intelligence, each reminds us that effective protection begins long before a crisis unfolds. The common thread is not tactics. It is judgment.

As editors, we believe that judgment will become the defining characteristic of the next generation of protection professionals. Technical skills will always matter, but they are not enough on their own. The professionals who will shape the future of this field will be those who can connect information across

disciplines, identify patterns others overlook, and make sound decisions in environments defined by uncertainty.

Ultimately, that is what this journal seeks to encourage. We hope these pages contribute to better practitioners and to a stronger profession, one that continues to embrace scholarship, welcomes thoughtful debate, and never loses sight of its fundamental purpose. Because, now more than ever, protection begins with understanding.

Treston Wheat, PhD
***Editor-in-Chief,* CPSJ**

Charles Randolph
Fred Burton
Charles Tobin
Rachael Frost
Samantha Newbery, PhD
Erin Rowland Carlin, PhD
***Editorial Staff Members*, CPSJ**

Research Articles

Fight or Flight: Use of Force Issues for Private Protection Personnel

Frederic Bruno and Elise T. Carlson, EdD

Executive Summary

The purpose of this paper is to clarify how statutes and case law affect the ability of protection personnel to safeguard their charges from physical harm. Minnesota Statutes establish that peace officers employed by law enforcement agencies are governed by § 609.066 (Authorized Use of Deadly Force by Peace Officers). Other statutes permit private individuals to use reasonable force to defend themselves, others, or property, under certain circumstances. However, Minnesota case law has long imposed a duty to retreat on private citizens before taking most defensive actions. In addition, Minnesota Statutes define protection personnel, such as security guards and protective agents, as individuals tasked with "preventing" crimes or "protecting" persons, thereby granting them the authority to act. This paper concludes that private protection personnel are governed by Minnesota Statutes §§ 609.06 and 609.065, and that the duty to retreat depends on the protection personnel's perception of the client's ability to retreat from danger.

Acknowledgements
Thank you to Paul Gherardi and Scott Mueller for contributing their expertise. Thank you also to Richard Hodsdon and John Sonsteng for providing their support.

Introduction: The Problem

As political and economic landscapes evolve in the United States, more incidents of violence against high-profile individuals arise. One study found that the number of federal charges for threats against public officials rose from 38 per year (in 2013-2016) to 62 per year (in 2017-2022).[i] However, the study tracked only the number of federal charges, not the number of all credible threats, which increases the number. In 2025, the U.S. Capitol Police anticipate they will investigate about 14,000 threats, which reflects a 950% increase from 2016.[ii] In response, the U.S. House of Representatives has doubled the amount of the lifetime residential security stipend to $20,000 and provided an additional $5,000 per month through the end of 2025.[iii] Additionally, because these numbers do not account for threats against private persons, such as CEOs and celebrities, nor any state charges, the true numbers of threats against high-profile individuals are necessarily much higher. In Minnesota, the June 2025 assassinations of Minnesota legislators raised concerns about safety of local public officials.

These high-profile individuals seek defense from such threats by hiring protection personnel. Yet, in Minnesota, a combination of statutory and case law creates confusion about exactly when and how protective personnel can act. This paper analyzes current information to clarify—at least somewhat—how protection personnel should act under Minnesota law. First, this paper will review the definitions of various protection personnel. Second, this paper will examine the laws regarding defense of self and others. Third, this paper will evaluate the meaning of "reasonable" as it applies to the actions of protection personnel. Fourth, this paper will review the definition of "weapon." Finally, this paper will provide a quick

reference guide to each of the previous topics. Though the main analysis will focus upon the law as it applies to non-police protection personnel, the analysis will also touch upon the law as it applies to protection personnel who are currently employed by a law enforcement agency. In either case, it is self-evident that protection personnel are employed entirely for the defense of others, which hence prescribes the scope this paper.

The Law

The law regarding defense of others in Minnesota arises from both statutory and case law.

Statutory definitions

Minnesota Statutes provide definitions for protection personnel, as well as defense of self and others. These definitions create the foundation of the understanding of protection and defense.

Protection personnel

Under the Minnesota Statutes, protection personnel can be grouped into three categories: (1) peace officers, (2) security guards, and (3) protective agents. This paper only briefly touches upon private detectives because the statutory definition does not provide for private detectives to engage in protective action.

a. Minn. Stat. § 626.84 – Peace officer

In relevant part, Minn. Stat. § 626.84 states that a peace officer is "an employee or an elected or appointed official of a political subdivision or law enforcement agency who is licensed by the board, charged with the prevention and detection of crime and the enforcement of the general criminal laws of the state and who has the full power of arrest."[iv] This definition highlights that a peace officer is (a) an employee or official of (b) a law enforcement agency. The peace officer is also (c) licensed by the board, (d) charged with preventing crime and enforcing laws, and (e) empowered to arrest. In short, a peace officer must be currently *employed* by a law enforcement agency.

b. Minn. Stat. § 326.32 – Security guard

Minn. Stat. § 326.32 states that a security guard is "a person who wears or carries any insignia that identifies the person to the public as security, who is paid a fee, wage, or salary to" prevent trespass or theft, protect individuals from bodily harm, or enforce the employer's policies to reduce crime, among other tasks.[v] Additionally, Minn. Stat. § 626.88 states that a security guard does not include "unarmed security personnel."[vi] It also states that security guards may wear uniforms that are any color "other than those specified for peace officers."[vii] A security guard is thus distinguishable because he (a) carries an insignia or wears a uniform, (b) is armed, and is (c) paid (d) to provide security in various forms.

c. Minn. Stat. § 326.338 – Protective agent

Minn. Stat. § 326.338 states that a protective agent is a "person who for a fee, reward, or other valuable consideration" protects people or their property, recovers property, responds to an alarm, or provides armored car services, among other tasks.[viii] This statute establishes that a protective agent (a) is paid (b) to protect people and property.

d. Minn. Stat. § 326.338 – Private detective

Minn. Stat. § 326.338 states that a private detective is someone who "for a fee, reward, or other consideration" investigates crimes, identity, character, affiliations, conduct, the recovery of property, and other matters.[ix] A private detective is distinguishable from the others because he (a) "investigates," rather

than “protects” or “prevents,” which indicates that a private detective is not part of the protection personnel categories.

Figure 1 displays the differences in the four categories.

Figure 1 – Comparison of statutory definitions of categories of protection personnel

Category	Employment	Powers	Armed	Uniformed
Peace officer	Law enforcement agency	Arrest, prevent crime, enforce laws	Yes	Yes
Security guard	Private	Prevent trespass, theft, bodily harm, enforce employer’s policies	Yes	Yes
Protective agent	Private	Protect people and property, provide protective services	Not defined	Not defined
Private detective	Private	Investigate crimes, credibility, conduct	Not defined	Not defined

These key statutory differences among the categories are important in the analysis of defense laws:

1. The peace officer is employed by a law enforcement agency.
2. The peace officer has the full power of arrest.
3. Both peace officers and security guards are presumed armed.
4. Both peace officers and security guards must display insignia or wear uniforms to inform the public of their role.
5. Peace officer, security guard, and protective agent definitions provide that such persons are to “prevent” crimes or “protect” persons, which grants them the power of action.
6. The private detective definition does not include any statement of “prevent” or “protect,” only “investigate.”

These differences among the categories factor into how each group can provide defensive protection to individuals. In practice, however, protective agents and security guards undergo the same licensing requirements and perform the same tasks.[x] Notably, a private detective does not have the statutory power of protection and, as such, may not engage in protective services for others under a private detective license.[xi] Therefore, much of this paper applies to only protective agents and security guards, who are herein collectively referred to as “protection personnel.”

Licensing requirements for protection personnel

The Minnesota Board of Private Detective and Protective Agent Services (PDB), as established by Minn. Stat. § 326.33, licenses protective agents/security guards and private detectives.[xii] Individuals, partnerships, corporations, and LLCs can apply for these licenses. Some requirements include a $10,000 surety bond and being free of felony convictions. The experience requirements are as follows:

> **PROTECTIVE AGENT**: An Individual (sole proprietor), or the Qualified Representative (and Minnesota Manager for an out-of-state applicant), must be able to document a minimum of 6,000 hours of security/protective employment experience in one or more of the following:
>
> - Employed in a protective/security capacity with a licensed protective agent, or in a protective/security for investigative capacity for a licensed private detective.
> - Employed in a protective/security or investigator capacity with a U.S. government investigative service.
> - Employed in a protective/security or investigator capacity with a city police department or sheriff's office.
> - Be employed in an occupation the board finds equivalent in scope, responsibility and training as one of the specific occupations listed above.
>
> Note: Each of the protective agent employment items referenced above must include experience in security systems, audits, and supervision of security personnel.
>
> **PRIVATE DETECTIVE**: An Individual (sole proprietor), or the Qualified Representative (and Minnesota Manager for an out-of-state applicant), must be able to document a minimum of 6,000 hours of investigative employment experience in one or more of the following:
>
> - Employed as an investigator with a licensed private detective/investigative agency.
> - Employed as an investigator with a U.S. government investigative service.
> - Employed as an investigator for a city police department or sheriff's office.
> - Be employed in an investigative occupation the board finds equivalent in scope, responsibility, and training as one of the specific occupations listed above.[xiii]

Further, applicants must complete background checks and specific board-required training in topics related to their specialties prior to taking assignments.[xiv]

Defense of Self and Others

This section introduces the three main statutes that lay the groundwork for defense of self and others in Minnesota. Because the statutes do not grant the private detective the power of defense, the following sections do not apply to private detectives.

a. Minn. Stat. § 609.06 – Authorized use of force

Under Minn. Stat. § 609.06, a public officer (including a police officer, but not a security guard or protective agent[xv]) may use reasonable force in conducting their duties. A private citizen (including a security guard or protective agent) may use reasonable force to protect himself, another, or property, only under certain conditions, such as “resisting or aiding another to resist an offense against the person” or “assisting the person in lawful possession” of real or personal property.[xvi] The statute also provides that a person may use reasonable force when arresting another “in the cases and in the manner provided by law.”[xvii]

Key elements of this statute are that (1) force must be reasonable and that (2) the actor reasonably believes dangerous circumstances exist, whether the actor is a public officer or private citizen. The statute also lays out that (3) an actor may resist on his own behalf or (4) aid another in resisting, whether for offenses against (5) the person or (6) real or personal property. Therefore, Minn. Stat. § 609.06 clearly provides that any person can defend himself or another, as well as real and personal property, against offense, interference, or trespass; however, such use of force must be "reasonable," which is less clear (see section II(B)3).

b. Minn. Stat. § 609.065 – Justifiable taking of life

Minn. Stat. § 609.065 establishes boundaries for instances in which an actor is justified in taking the life of another. This statute establishes that (1) intentional taking of life is only permissible when (2) the actor reasonably believes he or another is at risk of (3) great bodily harm or death. The actor may also take a life if he is (4) preventing a felony commission in the actor's place of abode.[xviii]

Therefore, Minn. Stat. § 609.065 provides that an actor can take a life when protecting himself or another from great harm, as long as he reasonably believes that harm to be real. The term "reasonable" is discussed further in section II(B)3.

c. Minn. Stat. § 609.066 – Authorized use of deadly force by peace officers

Finally, Minn. Stat. § 609.066 defines when a peace officer may use deadly force. It establishes that a peace officer's (1) intentional taking of life is only permissible when (2) the peace officer reasonably believes he or another is at risk of (3) great bodily harm or death.[xix] This statute, though similar to § 609.065, establishes a further restriction upon peace officers: rather than simply requiring that the peace officer himself see the situation as reasonably dangerous, it requires that (4) the peace officer use judgment that is reasonable to other peace officers in the same situation.[xx] The statute thus implies that peace officers will be held to a higher objective standard—the standard of their training and experience—in determining what danger and actions are "reasonable" under the Fourth Amendment's "objective reasonableness" standard.[xxi] The factors that an objectively reasonable officer must believe to be true, if faced with the same situation, are that the force is necessary:

> (1) to protect the peace officer or another from death or great bodily harm, provided that the threat:
>
> (i) can be articulated with specificity;
>
> (ii) is reasonably likely to occur absent action by the law enforcement officer; and
>
> (iii) must be addressed through the use of deadly force without unreasonable delay; or
>
> (2) to effect the arrest or capture, or prevent the escape, of a person whom the peace officer knows or has reasonable grounds to believe has committed or attempted to commit a felony and the officer reasonably believes that the person will cause death or great bodily harm to another person under the threat criteria in clause (1), items (i) to (iii), unless immediately apprehended.[xxii]

Additionally, according to the Minnesota Board of Private Detective and Protective Agent Services (PDB), a (1) current peace officer, who is (2) employed by a law enforcement agency, but (3) is acting strictly in a private protective capacity (4) while wearing an official agency uniform, will be held to the standard in § 609.066 if an incident occurs.[xxiii] Because peace officers are held to the standard in § 609.066, the following case law is less applicable to peace officers than to non-peace officers.

Statutes allow protection personnel to use reasonable force in specific situations
In sum, protection personnel—namely, security guards and protective agents—are regulated by § 609.06 and § 609.065. These statutes allow such protection personnel to use reasonable force to assist others in preventing (1) bodily harm, (2) interference with property, and (3) the commission of a felony in the home.

Note: The statutory term "actor" is used interchangeably with "defender" in the following sections.

Case Law

The Minnesota Statutes regarding defense of self and others leave much room for interpretation. Through their holdings, the courts have refined the meanings of the statutes, to include creating four elements of self-defense within Minn. Stat. § 609.06, subd. 1(3):

1. [T]he absence of aggression or provocation on the part of the defendant;
2. the defendant's actual and honest belief that he or she was in imminent danger of death or great bodily harm;
3. the existence of reasonable grounds for that belief; and
4. the absence of a reasonable possibility of retreat to avoid the danger.[xxiv]

Though the duty to retreat does not appear in the above-referenced statutes, the judiciary created the duty to retreat through case law. The duty-to-retreat doctrine has remained one of the elements of self-defense for years, and a recent legislative attempt to negate the duty to retreat failed to pass.[xxv] Therefore, the duty to retreat is active under current case law.

These four judicially-created elements apply to all non-peace-officer occurrences of defense of self and others in Minnesota, except that there is no duty to retreat within one's home. This paper presumes that the first three elements are met through appropriate behavior by protection personnel. Here, the question is when protection personnel may defend their charges, and when protection personnel must retreat. Therefore, the cases will first focus upon the duty to retreat while in public. Then, the cases will focus upon defense in the dwelling.

Defense in Public
While in public in Minnesota, a defender is always subject to duty-to-retreat considerations when reasonably possible. If a defender claims defense of self or others, and provides reasonable evidence to support the claim, the State must disprove one or more of the four elements of self-defense beyond a reasonable doubt.[xxvi] The fact-finder, such as the jury, determines whether the possibility of retreat was reasonable in that case.[xxvii] If the fact-finder determines that retreat was reasonable, then the defender will fail to meet the fourth element of defense, and likely will be found guilty of whichever crime with which he is charged.

Defense of Self
When defending oneself, a defender must retreat if possible. In *Blevins*, the defendant did not attempt to retreat, but, instead, brandished a machete at the aggressors.[xxviii] The Supreme Court of Minnesota affirmed the jury's finding that the defendant could have backed away from his aggressors while keeping an eye on them; additionally, it stated that the aggressors turned their backs on the defendant, which also provided the defendant with a chance to retreat.[xxix] Because the defendant did not use any opportunity to retreat, his claim of self-defense failed.

Protection personnel, by definition, are hired to protect others. However, if the "other" (one's charge) has safely retreated, the situation switches to self-defense. Then, the protection personnel must also retreat (if reasonable) before engaging in self-defense.

Defense of Others

In Minnesota, if a defender is defending another, the requirement of the duty to retreat still rests upon the four elements listed for self-defense. However, the actual duty to retreat is modified to be based upon whether the *person-in-peril* is reasonably able to retreat, rather than whether the defender is reasonably able to retreat, because requiring the defender to retreat would defeat "the very purpose of a defense-of-others claim."[xxx] In *State v. Valdez,* the Court defined the elements of defense-of-others to include:

1. A defendant must subjectively believe that the *person in peril* has no reasonable possibility of safe retreat, and
2. that belief must be objectively reasonable based on the information available to the defendant at the time that they used force to defend the person in peril.[xxxi] (Emphasis added.)

The Court stated that the perspective of the defender is appropriate for determining whether the person-in-peril is able to retreat; this is because it would be unrealistic to ask the defender to step into the place of the person-in-peril after the fact.[xxxii] Though the Court did not provide details about the second element of defense-of-others, the element appears to align with the third element of self-defense, which requires "reasonable grounds for that belief" that danger was imminent.[xxxiii] This requirement for the defendant's subjective in-the-moment belief to be objectively reasonable to others highlights that a defender's actions will only be defensible if they fall within the realm of general reasonableness.

In *Valdez*, the defendant protected his stepbrother. The aggressor, defendant, and stepbrother had spent an hour and a half together, playing pool in the defendant's garage. The defendant and stepbrother testified that the aggressor had been behaving erratically throughout the evening. Then, the aggressor threatened to kill the defendant and stepbrother. The defendant revealed his gun but did not point it at the aggressor. The aggressor lunged at the stepbrother, who hit the aggressor with a pool cue. The aggressor then tackled the stepbrother, held him down, and choked him. At this point, the stepbrother had no reasonable means of escape, and the defendant fatally shot the aggressor.[xxxiv]

The Court held that the fact-finder must "focus on the moment that the defendant elected to use force" when deciding the reasonableness of the action, not any moments prior.[xxxv] In *Valdez*, the defendant and stepbrother both admitted they could have retreated in moments prior to the time at which the aggressor choked the brother, but that did not prevent the potential validity of the defendant's defense-of-others claim.[xxxvi] Therefore, it is possible that a jury could find the defendant's actions—in the moment of the stepbrother's distress—reasonable.

Similarly, the Court determined that a jury could find that a defendant acted reasonably in shooting aggressors who were thirty feet away. In *State v. Baker,* the Court stated that the defendant knew that the persons-in-peril could not retreat because the aggressors had stolen their car keys, and the persons-in-peril were in the line of gunfire.[xxxvii] Therefore, it is possible that a jury would find that, both subjectively and objectively, the defendant believed he needed to protect the persons-in-peril.

Protection personnel should carefully assess whether the person-in-peril is able to retreat. If the person-in-peril cannot reasonably retreat, the protection personnel may defend the person-in-peril. Additionally, protection personnel should continue to assess the situation as it unfolds. If the aggressor backs off, or if

the person-in-peril gains an opportunity to retreat, the protection personnel should also retreat. Case law suggests that it is not advisable for protection personnel to give chase to an aggressor once the person-in-peril is safe.

However, Minn. Stat. §§ 629.37-39 provide that private citizens may arrest another for public offenses and felonies; if there are multiple protection personnel, and one can reasonably pursue the offender with the purpose of arresting him, it may be reasonable to do so.[xxxviii] Additionally, Minn. Stat. § 609.06, subd. 1(2), authorizes a citizen making an arrest to use reasonable force to effect the arrest.[xxxix]

Defense of Property

Minn. Stat. § 609.06, subd. 1(4), provides that a person may protect his own, or assist someone else in their protection of, personal property from "trespass" or "unlawful interference."[xl] *Baker* established that an attempt to recover personal property—as the aggressors are escaping with the property—falls within the description of an "ongoing" robbery.[xli] If a defender resists the robbery as it is ongoing, it falls under the protections of Minn. Stat. § 609.06, subd. 1(4). However, the boundary between an ongoing robbery and one that is complete is not clearly defined.

Protection personnel are often charged with defending property, whether carried by the owner or transported on behalf of the owner. While the statutes provide that such protection personnel can act to prevent theft or loss, it is unclear exactly when and how protection personnel can act. Under the current statutes and cases, protection personnel should consider the level of harm to the property before acting, and should only use defense that is reasonable in preventing further loss. Current law suggests that the preferred course of action is to take the least harmful measures necessary to prevent the loss.

Defense in the Dwelling

If a person can reasonably retreat into the dwelling, then, as a matter of law, use of force outside the dwelling is unreasonable. If a person is inside the dwelling, then the person may use reasonable force to defend, without any duty to retreat (unless the aggressor also has property rights to the dwelling, see section c. Defense of dwelling).[xlii]

Definition of "dwelling"

Defense of self or others in the dwelling is strictly limited to areas that are under the exclusive control of the property owner. In a 2006 case, the Court upheld a finding that the front deck of a dwelling counted as part of the dwelling as a matter of law, and that the defender did not have a duty to retreat from the deck.[xliii] The deck is considered part of the dwelling because it is an "attached appurtenance" of the dwelling.[xliv] However, general "curtilage," which is the area immediately around the dwelling, is *not* considered part of the dwelling.[xlv] Therefore, a defender cannot reasonably use force while standing just outside a window, or among bushes that line the outer wall of the house.

If a defender stands in the doorway of the dwelling, rather than inside it, the question of whether this position qualifies as being "within the dwelling" may be left to the fact-finder. Case law indicates the determination depends on whether there is an immediate threat of forced entry by the aggressor and whether the aggressor is located on a part of the dwelling (such as a porch) or merely within the curtilage, yard, or driveway (Court of Appeals, non-precedential).[xlvi] If the aggressor (1) occupies a part of the dwelling, and (2) physically poses a threat of entry, the defender may be justified in claiming defense from the doorway. By contrast, if either an aggressor or defender is (1) only in the curtilage of the dwelling, the defender must retreat to the dwelling itself; for example, if the defender is in the doorway, but the aggressor is in the driveway, the defender will likely be unable to claim defense of dwelling, as the

driveway is not considered part of the dwelling.[xlvii] The same reasoning applies to apartment hallways: a shared hallway is not part of a dwelling, because the defender can retreat inside his or her apartment and does not maintain exclusive control of the hallway.[xlviii]

Defense of self or others

When a defender is truly inside the dwelling, a defender does not have a duty to retreat, as the dwelling is viewed as the safest place and the location to which one would retreat if an attack began outside.[xlix] While defending himself or another from bodily harm, this applies even if the aggressor is a co-resident or other invited guest—the defender does not have to retreat within the dwelling.[l] However, the defender must still use reasonable force in his defense, and only when there is no reasonable alternative to the use of force. When defending another in one's own dwelling, a defender also does not have a duty to retreat. Deadly force is only authorized if the defender has a reasonable belief that he or another is in danger of "great bodily harm or death."[li]

Protection personnel are present in another's dwelling by invitation of, and payment by, the owner of the dwelling, which extends the "safest place is home" concept to the protection personnel.[lii] The client expects that the protection personnel will defend the residents of the dwelling, if necessary. Therefore, because the protection personnel are extended the protection of the "home" while inside the dwelling, protection personnel do not have a duty to retreat while defending themselves or others with reasonable force.

Defense of Dwelling

Defense of the dwelling requires that the aggressor be someone who does *not* have property rights to the dwelling. If both parties are co-residents, then they both have property rights to the dwelling.[liii] Therefore, a person can only defend the dwelling against an *unauthorized* intrusion, or trespass.[liv]

A defender must still use reasonable force in defending the dwelling.[lv] In a clarification that allows for freedom of "how" a defender uses force, the Supreme Court of Minnesota stated that defending the dwelling is not an "offensive purpose," but, rather, a defensive one; yet, the Court also recognized that, while defending, it might be "more reasonable for a person to advance towards or retreat from a danger . . . in different circumstances," and that such analysis should be left to a jury.[lvi] This statement highlights that the way in which someone defends the dwelling is open to the interpretation of reasonableness, but that minimal force should be used to prevent the danger.

As the Court of Appeals of Minnesota stated in the *McCuiston* case (non-precedential), Minn. Stat. § 609.065 must be read in conjunction with § 609.06 to understand that only reasonable force may be used to prevent a felony.[lvii] For example, the prevention of a felony does not always allow for force because (1) preventing a non-physical felony like "insurance fraud" would (2) not necessitate force.[lviii] This decision, while not binding, aligns with other holdings that limit force to reasonable applications, and suggests that deadly force to prevent a felony must also be reasonable.

Deadly force may not be used in defense of dwelling unless the defender holds a reasonable belief that it is necessary to prevent the commission of a felony within the dwelling; however, there is no requirement that the defender fear great bodily harm or death before using deadly force to protect the dwelling from the commission of a felony.[lix] The Court delineated three factors that a jury must determine when assessing a killing during a defense-of-dwelling claim:

1. At the time the defendant used deadly force against the victim, was the defendant preventing the commission of a felony in his or her home?
2. Was the belief reasonable under the circumstances?
3. Was the use of deadly force reasonable under the circumstances in light of the danger then to be apprehended?[lx]

Protection personnel are present in another's dwelling by invitation of, and payment by, the owner of the dwelling. Under § 609.06, subd. 1(4), a non-owner is permitted to assist a "person in lawful possession" of real or personal property.[lxi] A non-owner that is assisting an owner may use reasonable force to prevent trespass or "other unlawful interference" with such property.[lxii] Therefore, protection personnel may use reasonable force to protect the dwelling, as assistance to the owner, as long as the aggressor does not have rights to the dwelling.

Definition of "Reasonable"

The statutes and case law surrounding self-defense and defense of others include the term "reasonable" at almost every step. Based upon the decisions in case law, it appears that "reasonable" aims to curb the use of force where none is needed, or to limit the degree of force to the minimum amount needed to ensure the defender's safety. The definition of "reasonable" force is that it "must not exceed that which appears to be necessary to a reasonable person under similar circumstances." [lxiii] Therefore, the reasonableness of a defender's force is left to a jury to determine. Because the determination of "reasonable" is left to a jury, it is not possible to describe a bright-line definition; however, if the court finds that there is no way a jury could find the force reasonable, then the court may make the determination that the force was unreasonable as a matter of law.[lxiv]

For example, in *Baker*, the Court of Appeals concluded that the defender's use of force was unreasonable as a matter of law.[lxv] This was based upon the facts that the defender shot a thief eleven times and killed him, which the Court of Appeals felt no jury could find reasonable. However, the Supreme Court reversed this holding and remanded the case because, upon further analysis of the evidence, it acknowledged that it was possible for a reasonable jury to find the degree of the use of force reasonable.[lxvi] As of the writing of this paper, the case has not yet been retried with a jury. Hence, under *Baker*, it may be risky for a judge to exclude, in an *in limine* order, a defendant's theory of defense. Protection personnel should keep in mind that "reasonable" appears throughout all aspects of defense.

Figure 2 summarizes the ways in which "reasonable" appears.

Figure 2 - Categories in which "reasonable" appears as a modifier for actions

Subjective Belief by Actor	**Use and Degree of Force**
1. Minn. Stat. § 609.06: actor **reasonably** believes circumstances exist 2. Minn. Stat. § 609.065: actor **reasonably** believes exposure to great bodily harm or death 3. Minn. Stat. § 609.065: actor **reasonably** believes exposure to felony in dwelling	1. Minn. Stat. § 609.06: **reasonable** force may be used 2. Deadly force - bodily (case law): use of deadly force **reasonable** with exposure to great bodily harm or death 3. Deadly force - dwelling (case law): use of deadly force **reasonable** under circumstances to prevent felony

Objective Grounds for Actor's Belief	Possibility of Retreat
1. Self-defense (case law): **reasonable** grounds for honest belief of danger 2. Defense of others (case law): belief that person-in-peril could not reasonably safely retreat must be objectively **reasonable** based on actor's information at the time 3. Defense of dwelling (case law): belief of commission of felony **reasonable** under the circumstances	1. Self-defense (case law): absence of **reasonable** possibility of retreat 2. Defense of others (case law): actor's belief that person-in-peril could not **reasonably** safely retreat

Protection personnel must assess situations quickly and fluidly and ensure that their choices to (1) use force and (2) how much force to use are within the realm of what a jury could find reasonable.

Brandishing a weapon can be considered assault-fear

The requirement to retreat applies both when the defender causes bodily harm to the aggressor, and to when the defender commits assault-fear with a dangerous weapon, as the Court delineated in *Blevins*.[lxvii] The Court in *Blevins* emphasized that its holding was a narrow application of the law to assault-fear with a dangerous weapon, which is a "device designed as a weapon and capable of producing death or great bodily harm . . . or other device . . . calculated or likely to produce death or great bodily harm."[lxviii] The Court also emphasized that, if a defendant simply *prepared* to use a weapon, that would not be the same as *brandishing* the weapon with an intent to cause fear of great bodily harm.[lxix] Therefore, it appears that *preparing* does not constitute an action that would induce assault-fear, but *brandishing* would likely create a situation of assault-fear.

Outside of the narrow holding in *Blevins*, the Court has also decided cases in which dangerous weapons, other than firearms, were in question. The statute describes a dangerous weapon, in part, as a "device or instrumentality that, in the manner it is used or intended to be used, is calculated or likely to produce death or great bodily harm."[lxx] The Court has previously held that slapping, punching, and kicking can make one's hands and feet into dangerous weapons when used in "brutal and prolonged attacks against vulnerable and sometimes defenseless victims."[lxxi] In *Basting*, the Court further clarified that the manner of use is key. The defendant was accused of using his fist as a dangerous weapon because he was a professional boxer. However, the Court found that it is "not only the nature of the object itself, but also the manner in which it was used" that determines whether the object is a dangerous weapon in that scenario.[lxxii] Because the defendant in *Basting* had only briefly used his fists against someone of similar size, the Court found his use of his professionally-trained fists did not rise to the level of a dangerous weapon.[lxxiii]

Protection personnel, who are often armed with a firearm (a dangerous weapon), must use caution in preparing or brandishing such a firearm. Though there is no clear answer, it seems that simply moving a jacket aside to reveal a firearm in its holster may be considered "preparing" to use the weapon, as it is reasonable to believe that there is not yet imminent danger to the other party (for example, when the defendant first revealed his gun to the aggressor in *Valdez*).[lxxiv] However, once the defender brandishes the gun and aims it toward the aggressor, it is reasonable to believe that there is imminent danger to the

other party. Therefore, to avoid charges of assault-fear, it is in the protection personnel's best interest to retreat, if possible, prior to aggressively brandishing a weapon. If protection personnel engage in a physical altercation, they should keep in mind the reasonableness of their use of force to ensure that their professional training in hand-to-hand combat does not rise to the level of a dangerous weapon.

Conclusion

Under current statutory and case law, protection personnel are governed by Minn. Stat. § 609.06 and § 609.065, as well as elements defined by the Supreme Court of Minnesota in its holdings. While defending another, protection personnel should analyze the person-in-peril's ability to reasonably retreat to safety. If the person-in-peril can reasonably retreat, it is unreasonable for the protection personnel to use deadly force against an aggressor. If the person-in-peril cannot reasonably retreat, the protection personnel may use reasonable force against an aggressor, including deadly force, if necessary. While providing protection in the client's home, protection personnel may use reasonable force to protect both people and property without a duty to retreat. What is "reasonable" is left to a jury to decide, so protection personnel must use sound judgment when acting to protect clients.

Authors:
Frederic Bruno is an Attorney at Law with Bruno Law PLLC and a leading Minnesota lawyer for police and protective agents.

Elise T. Carlson, EdD is currently a law student at Mitchell Hamline School of Law and an adjunct professor.

Quick Reference Guide

Figure 3 - Reference guide for various protection scenarios

Where	Who	Duty to Retreat	Use of Force	Deadly Force
In public	Self-defense	Based on own ability to safely retreat	If reasonable, and reasonable degree	Reasonable exposure to great bodily harm or death
In public	Defense of another	Based on person-in-peril's ability to safely retreat, as assessed by the defender	If reasonable, and reasonable degree	Reasonable exposure to great bodily harm or death
In public	Citizen's arrest	May pursue immediately after offense	If reasonable, and reasonable degree	Reasonable exposure to great bodily harm or death
In dwelling	Self-defense	No	If reasonable, and reasonable degree	Reasonable exposure to great bodily harm or death

In dwelling	Defense of another	No	If reasonable, and reasonable degree	Reasonable exposure to great bodily harm or death
In dwelling	Defense of dwelling	No, unless aggressor has property rights	If reasonable, and reasonable degree	Only to prevent a [violent] felony

Endnotes

[i] Pete Simi, et al. "Rising Threats to Public Officials: A Review of 10 Years of Federal Data," *CTC Sentinel* 17 (May 2024): 20.
[ii] Kelly Kosuda, "Rising Threats Against Lawmakers Spur Urgent Calls for Security Upgrades," *NBC5*, September 11, 2025, https://www.mynbc5.com/article/rising-threats-against-lawmakers-security-upgrades/66056077.
[iii] Ibid.
[iv] Minn. Stat. § 626.84, subd.1 (2024).
[v] Minn. Stat. § 326.32, subd.13 (2024).
[vi] Minn. Stat. § 626.88, subd.1(c)(6)(iii) (2024).
[vii] Minn. Stat. § 626.88, subd. 2(b) (2024).
[viii] Minn. Stat. § 326.338, subd. 4 (2024).
[ix] Minn. Stat. § 326.338, subd. 1 (2024).
[x] Paul Gherardi, President, Empire Investigation & Protective Services, Inc., email message, September 25, 2025.
[xi] Ibid.
[xii] Minn. Stat. § 326.33 (2024).
[xiii] Minnesota Board of Private Detective and Protective Agent Services, "General Licensing Information," https://dps.mn.gov/about-dps/associated-boards-cmtes-and-task-forces/private-detective-and-protective-agents-board/license-holders/general-licensing-information.
[xiv] Minn. R. § 7506.2600 (2024).
[xv] Minn. Stat. § 609.415 (2024).
[xvi] Minn. Stat. § 609.06 (2024).
[xvii] Minn. Stat. § 609.06, subd. 1(2) (2024).
[xviii] Minn. Stat. § 609.065 (2024).
[xix] Minn. Stat. § 609.066 (2024).
[xx] Ibid.
[xxi] *Graham v. Connor*, 490 U.S. 386, 109 S. Ct. 1865, 104 L. Ed. 2d 443 (1989).
[xxii] Minn. Stat. § 609.066, subd. 2 (2024).
[xxiii] Scott Mueller, Deputy Superintendent of Investigative Services, Minnesota Bureau of Criminal Apprehension, email message, August 15, 2025.
[xxiv] *State v. Basting*, 572 N.W.2d 281, 285 (Minn. 1997).
[xxv] Tim Walker, "Bill to Expand Right to Self-Defense in Minnesota Fails House Vote," Minnesota House of Representatives, March 6, 2025, https://www.house.mn.gov/sessiondaily/Story/18572.
[xxvi] *State v. Johnson*, 719 N.W.2d 619, 629 (Minn. 2006).
[xxvii] *State v. Blevins*, 10 N.W.3d 29, 38 (Minn. 2024).

[xxviii] Ibid., 32.
[xxix] Ibid., 40.
[xxx] *State v. Valdez*, 12 N.W.3d 191, 197 (Minn. 2024).
[xxxi] Ibid, 199.
[xxxii] Ibid.
[xxxiii] *Basting*, 572 N.W.2d at 285.
[xxxiv] *Valdez*, 12 N.W.3d at 200 n.10.
[xxxv] Ibid.
[xxxvi] Ibid.
[xxxvii] *State v. Baker,* 13 N.W.3d 401, 411 (Minn. 2024).
[xxxviii] Minn. Stat. §§ 629.37-39 (2024).
[xxxix] Minn. Stat. § 609.06, subd. 1(2) (2024).
[xl] Minn. Stat. § 609.06, subd. 1(4) (2024).
[xli] *Baker,* 13 N.W.3d at 410.
[xlii] *State v. Glowacki*, 630 N.W.2d 392, 401 (Minn. 2001).
[xliii] *State v. Penkaty*, 708 N.W.2d 185, 207 (Minn. 2006).
[xliv] Ibid.
[xlv] Ibid.
[xlvi] *State v. McCuiston*, 514 N.W.2d 802, 803 (Minn. Ct. App. 1994).
[xlvii] *Penkaty*, 708 N.W.2d at 207.
[xlviii] *State v. Devens*, 852 N.W.2d 255, 259 (Minn. 2014).
[xlix] *Glowacki*, 630 N.W.2d at 401.
[l] Ibid.*,* 402.
[li] *State v. Pendleton*, 567 N.W.2d 265, 268 (Minn. 1997).
[lii] Scott Mueller, August 15, 2025.
[liii] *State v. Hare,* 575 N.W.2d 828, 832 (Minn. 1998).
[liv] Ibid.
[lv] *Glowacki*, 630 N.W.2d at 399.
[lvi] *State v. Carothers*, 594 N.W.2d 897, 904 (Minn. 1999).
[lvii] *McCuiston*, 514 N.W.2d at 806.
[lviii] Ibid., 805.
[lix] *Pendleton*, 567 N.W.2d at 268.
[lx] Ibid., 269.
[lxi] Minn. Stat. § 609.06, subd. 1(4) (2024).
[lxii] Ibid.
[lxiii] *Basting*, 572 N.W.2d at 286.
[lxiv] *Baker,* 13 N.W.3d at 411.
[lxv] *Baker,* 13 N.W.3d at 405.
[lxvi] Ibid., 411.
[lxvii] *Blevins*, 10 N.W.3d at 37.
[lxviii] Minn. Stat. § 609.02, subd. 6 (2024).
[lxix] *Blevins*, 10 N.W.3d at 38 n.9.
[lxx] MINN. STAT. § 609.02, subd. 6 (2024).
[lxxi] *Basting*, 572 N.W.2d at 284.
[lxxii] Ibid., 285.
[lxxiii] Ibid.
[lxxiv] *Valdez*, 12 N.W.3d at 194.

BAIP: A Motivational Taxonomy for Executive Targeting – Operationalizing Behavioral Threat Assessment in Corporate Protection (LatAm Emphasis)

Kevin E. Palacios

Abstract

The BAIP model (Behavioral Analysis of Indicators and Pathways - or - Beneficio–Agravio–Ideología–Psicopatología) is a specialized motivational taxonomy designed as an analytical-operational module within Behavioral Threat Assessment and Management (BTAM) for executive protection environments. Developed for corporate and high-net-worth (HNW) contexts—particularly in Latin America, where instrumental criminal motives (Benefit) are frequently prominent alongside grievance, ideology, and fixation/disorganization patterns—BAIP classifies observable behaviors to support hypothesis formulation, targeted information collection, and proportionate risk mitigation inside an Executive Protection Risk Management (EPRM) architecture. This paper outlines BAIP's doctrinal foundations, maps it to the Pathway to Violence, and provides operational artifacts (BAIP-OP gates/RACI; BAIP-X behavioral taxonomy; BAIP-VAL rubric; escalation matrix; case lifecycle). A retrospective validation study on 28 real/historical cases (LatAm-first prioritization, minimum two verifiable sources per case) provides exploratory evidence of classification clarity, hybrid-pattern recognition, and alignment with BTAM principles of early intervention, articulability, and proportionality. Findings underscore the importance of physical–digital convergence monitoring via Digital Shield (DS) and structured Protective Intelligence (PI)/Global Security Operations Center (GSOC) orchestration, including in AI-supported implementations. Within that architecture, the BAIP Model is part of the EPRM framework and provides the technical basis for this implementation.

Introduction

Executive Protection Threat Management in the contemporary corporate landscape faces a specific operational gap. Behavioral Threat Assessment and Management (BTAM) frameworks and guidance commonly emphasize a processes for identification, inquiry, assessment, and management of directed violence, but they rarely offer an EP-specific, memorable, and actionable taxonomy of predominant motivations tailored to executives targeted not as private individuals but as symbols or instruments of power, wealth, decision-making authority, or corporate conflict.[i] Generally, there is abundant general BTAM theory but insufficient operational methodologies that could be directly taught to, and executed by, Executive Protection teams in high-risk Latin American (LatAm) environments. Existing literature and case materials are heavily skewed toward "grievance" as a general driver; this focus, while valid in many U.S./European contexts, does not fully reflect the LatAm threat landscape where Benefit-driven instrumental criminality—extortion, coercion, tiger kidnappings, and strategic pressure on corporate assets—often constitutes the primary motivation.[ii]

BAIP (Behavioral Analysis of Indicators and Pathways - or - Beneficio–Agravio–Ideología–Psicopatología) does not attempt to replace BTAM frameworks. Its contribution is narrower and operational by providing executive protection teams with a memorable, behavior-anchored motivational taxonomy that (a) explicitly treats instrumental "Benefit" targeting as a first-class category (especially relevant in many Latin American executive risk environments), (b) standardizes how multidisciplinary corporate teams articulate a Primary/Secondary motivational hypothesis with an explicit confidence level, and (c) connects that motivational formulation to concrete operational artifacts (BAIP-X, BAIP-VAL, escalation levels, and case lifecycle states) suitable for governance review. Innovation is therefore framed as an applied integration. BAIP is a practical "why" module optimized for executive protection decision cycles, designed to reduce interpretive drift, accelerate disciplined information collection, and improve the defensibility of proportional controls.

The author developed BAIP to function as a motivational classification module inside a standard BTAM workflow, governed by an EPRM architecture. The four categories are deliberately simple and teachable, so Artificial Intelligence (AI) and human agents could be trained to team up, classify motivation consistently, communicate risk clearly, and select proportionate controls under real executive protection constraints—time pressure, incomplete information, and multidisciplinary coordination.

This paper delivers three contributions: (1) a complete doctrinal and operational presentation of BAIP as published in the EPRM framework; [iii] (2) a reproducible retrospective validation methodology and descriptive results from a 28-case corpus (LatAm priority); and (3) explicit integration guidance within EPRM, highlighting the non-negotiable roles of Digital Shield (DS), Protective Intelligence (PI), and the Global Security Operations Center (GSOC) IA agents. The analysis maintains strict claim discipline: every factual statement about cases is supported by verifiable sources; facts are separated from interpretation; "psychopathology" is treated exclusively as an operational label for observable fixation/disorganization (never a clinical diagnosis); and all recommendations are risk-based and proportional.

Doctrinal Framework: BAIP within BTAM/EPRM

What BAIP Is / What BAIP Is Not

BAIP is a motivational taxonomy specialized for violence directed against executives in corporate and high-exposure contexts. It answers the question: "Why does this targeting appear to be occurring?" on the basis of observable, verifiable behaviors. It is explicitly not:

- a clinical diagnostic tool
- a deterministic predictor of violence
- a replacement for the overarching BTAM process (Identify–Inquire–Assess–Manage)
- justification for disproportionate measures absent credible threat, protectee profile, and operational context

Instead, BAIP operates as an analytical module embedded inside BTAM/EPRM. BTAM governs the full case lifecycle. EPRM supplies governance, decision authority, and execution. BAIP supplies structured motivational formulation to orient information collection, hypothesis testing, and selection of proportional controls.[iv3]

Behavioral Principles

The model rests on seven doctrinal principles:

1. **Behavioral principle:** exclusive reliance on observable, verifiable, documentable conduct—no psychological profiling.
2. **Separation of analysis:** facts observed vs. analytical interpretation vs. uncertainty/confidence level.
3. **Progression:** violence as dynamic process (Pathway to Violence heuristic).
4. **Multicausality:** Primary + Secondary motivation + confidence level (High/Medium/Low).
5. **Early intervention:** manage concern signals before verified intent/capability.
6. **Articulability:** every decision evidence-based and explainable (minimum evidence standard per BAIP-OP gate).
7. **Proportionality:** measures calibrated to real risk (protectee profile, credible threats, operational context).

These principles align directly with NTAC, DHS BTAM, and Deisinger standards while adding EP-specific clarity for corporate targeting.

Operational Definitions and EP Implications

- **B (Beneficio / Benefit):** The executive is used as an efficient means to obtain money, coercion, influence, or strategic advantage. **EP implication:** harden exposure, residence, and mobility; countersurveillance; crisis/law enforcement coordination as thresholds are met.
- **A (Agravio / Grievance):** A persistent perception of injustice, humiliation, or loss attributed to the executive or organization, personal – traditional grievance. **EP implication:** narrative tracking; contact control; HR/legal coordination; proximity/access evaluation; monitoring for leakage.
- **I (Ideología / Ideology):** The executive is treated as a symbol of a system, cause, or structure the actor considers legitimate to attack. **EP implication:** campaign/event monitoring; residence hardening; and physical–digital convergence management via Digital Shield.
- **P (Psicopatología / Psychopathology — operational label, non-diagnostic):** Observable patterns of fixation, perseveration, disorganization, incoherence, or boundary-violating contact that do not presently fit a clearly structured Benefit/Grievance/Ideology driver, or that remain ambiguous due to insufficient evidence. **EP implication:** strict contact/access management; exhaustive documentation and evidence preservation; structured consultation (legal, HR, and—when proportional and appropriate—behavioral health/subject-matter experts and/or law enforcement). This label is used for operational risk description only and must never be treated as clinical diagnosis.

Table 1. BAIP Categories: Operational Definitions and Executive Protection Implications

Code	Category	Operational definition	Dominant indicators	Protection implication
B	Beneficio / Benefit	The executive is used as a means to obtain money, power, coercion, or strategic advantage.	Kidnapping, extortion, blackmail, strategic coercion, targeting based on real or perceived ability to pay.	Hardening of exposure, residence, and mobility; countersurveillance; coordination with crisis management/law enforcement.
A	Agravio / Grievance	Violence is fueled by a persistent perception of injustice, humiliation, loss, or victimization attributed to the executive or the organization.	Blame narratives, resentment, externalization, leakage, and progression toward punishment.	Narrative tracking; contact control; coordination with HR/legal; proximity and access assessment.

I	Ideología / Ideology	The executive is treated as a symbol of a system, cause, or structure the actor believes is legitimate to attack.	Anti-corporate framing, single-issue extremism, radicalized activism, coordinated campaigns, glorification or moral legitimization of violence.	Monitoring of campaigns, events, home exposure, reputation, travel, and physical–digital convergence.
P	Psicopatología / Psychopathology (operational label; non-diagnostic)	The analyst does not diagnose the subject; observable patterns of persistent fixation, disorganization, apparent incoherence, or opportunism without a clearly structured grievance/benefit/ideology driver are documented.	Obsessive persistence, repetitive contact, strange or delusional content, stalking-like behavior, opportunism enabled by target vulnerability.	Strict contact and access management; exhaustive documentation; clinical/legal consultation when warranted.

Behavior & Progression: BAIP Mapped to Pathway to Violence

BAIP adopts the widely validated Pathway to Violence model (Calhoun & Weston, 2003; CISA/NTAC adoption) as a non-deterministic heuristic.[v] The six stages— Grievance, Indicators/trigger, Ideation, Research & Planning, Preparation, Probing & Breaching, Attack—allow temporal ordering of evidence and identification of intervention windows. EPRM provides the full BAIP-mapped matrix (reproduced in Appendix). An individual's motivation often shapes the behaviors they display before an incident occurs. Cases driven primarily by grievance or practical objectives (B-type) tend to involve deliberate reconnaissance, information gathering, and the exploitation of vulnerabilities. Cases driven by attachment or obsession (A-type) are more likely to involve online leakage, escalating narratives, and efforts to increase contact or proximity to the target. Ideologically motivated actors (I-type) often engage in coordinated online campaigns, harassment, or doxxing, while persistent fixation cases (P-type) frequently involve repeated, disorganized attempts at communication. Because digital platforms have accelerated and exposed many of these early warning behaviors, robust digital monitoring and protection measures are increasingly essential. (The use *protectee* means the protected principal within scope.)

Audit-Ready Operational Package

BAIP is fully operationalized through five integrated tools:

- **BAIP-OP**: Six-gate workflow (Triage Classification BAIP-VAL Communication & Escalation Treatment Monitoring & Closure) with Responsible, Accountable, Consulted, Informed (RACI) matrix and minimum evidence standard per gate.
- **BAIP-X**: Behavioral taxonomy across Physical (F1–F5), Digital (D1–D6), Hybrid (H1–H3) domains (detailed summary in Appendix).
- **BAIP-VAL**: Structured rubric requiring observed conduct, signals, domain/family, target, concern elicited, BAIP Primary/Secondary + confidence, capability, pathway stage, impact, interpretation, recommendation, decision/approver.
- **Escalation Matrix (0–4)**: Defined activation criteria, minimum actions, recipients, and evidence required.

- **Case Lifecycle**: Standardized states (OPEN TRIAGE FULL ASSESSMENT MITIGATION MONITORING CLOSED) with entry/exit criteria, owner, review frequency, and mandatory after-action review (AAR)/corrective and preventive actions (CAPA).

These artifacts convert BAIP from descriptive taxonomy to repeatable, auditable component of EPRM governance.

Retrospective Validation Methodology

To test BAIP's operational utility as a motivational module within BTAM/EPRM, a retrospective validation study was conducted on a corpus of 28 real/historical cases of executive-directed targeting. The methodology was designed for reproducibility, inter-analyst consistency, and strict adherence to the behavioral principles codified in the source BAIP Model document.

Corpus design and selection rules

Cases were prioritized per the LatAm-first rule: (1) Latin America (observable behaviors in executive extortion, coercion, *escraches* (public shaming protests), or hybrid campaigns); (2) United States; (3) other jurisdictions.

For replicability, a case is defined as a discrete episode of executive-directed targeting (physical, digital, or hybrid) with enough publicly verifiable detail to code at least one BAIP-X behavioral family and to assign a BAIP Primary/Secondary hypothesis with an explicit confidence level. A verifiable source is defined as a primary or traceable secondary record that documents observable conduct (e.g., court filings/indictments, official law enforcement statements, or investigative reporting that cites primary documents), as opposed to rumor, anonymous social media claims, or uncorroborated commentary.

Inclusion required:

- Verifiable observable facts (what happened, channel, approximate timeframe, domain).
- Ability to code BAIP-X domain/family before assigning BAIP Primary/Secondary.
- Minimum two verifiable sources (court records, DOJ/indictments, official LE statements, or reputable investigative reporting linking to primaries).
- Separation of facts from interpretation; "Unknown / Insufficient evidence" applied where pre-incident leakage, capability, or exact pathway stage could not be confirmed from public records.

Exclusion criteria: rumor-based claims, insufficient behavioral granularity, or inability to distinguish facts from media speculation. The final corpus comprises 13 LatAm, 13 U.S., and 2 Other cases, balanced across typologies (insider/grievance, hostile campaigns, doxxing/hybrid, extortion/coercion, stalking, radicalized activism, crisis-related).

Source verification and coding procedure

1. **Facts-first extraction:** objective narrative of observed conduct (physical/digital/hybrid), channel, and temporal markers.
2. **BAIP-X coding:** domain (Digital D1–D6, Hybrid H1–H3, Physical F1–F5) and behavioral family.
3. **BAIP motivational hypothesis:** Primary + Secondary (if applicable) + confidence level (High/Medium/Low), justified solely by documented behaviors.
4. **BAIP-VAL population:** concern elicited, target of behavior, pathway stage (heuristic only when evidenced), capability, impact, and recommendation fields.

5. **Explicit separation:** facts recorded verbatim; interpretation labeled as analytical hypothesis with confidence. “P” assigned only for observable fixation/disorganization without clear B/A/I structure and never as clinical diagnosis.

The author coded the corpus and applied an internal quality assurance (QA) cross-check against BAIP doctrinal principles. Metrics evaluated: (a) classification clarity (ease of Primary/Secondary assignment post-BAIP-X); (b) hybrid frequency; (c) evidence constraints by region/typology; (d) alignment with Pathway to Violence stages. This approach mirrors BTAM standards (NTAC emphasis on corroboration, multi-source validation, and articulability) while testing BAIP’s added value in EP contexts.

Results

Distribution of BAIP Primary by region and typology

In the 13 LatAm cases, B (Beneficio) predominated in the corpus, reflecting instrumental criminal motives such as extortion and coercion as documented in official reporting and aggregated security analyses. These cases frequently involved hybrid convergence (H1/H2 families) where digital exposure facilitated physical probing or access-seeking. A (Agravio) appeared as Secondary in several cases, often layered on personal, labor-related, or reputational resentment. These findings should be interpreted as practice-based pattern observations, not as prevalence estimates.

In the 13 U.S. cases, A (Agravio) appeared most frequently as Primary in the corpus, consistent with grievance-fueled patterns in insider threats, hostile campaigns, and crisis-related events. The eBay cyberstalking campaign (2019) exemplifies A-dominant behavior: coordinated harassment (D1/H3) driven by perceived corporate injury, with corporate insiders as actors.[vi] Recent high-profile executive attacks and threat waves illustrate how grievance narratives and symbolic framing can rapidly shape post-incident targeting discourse, including copycat signaling and list-making behaviors in online spaces. In BAIP terms, such post-incident ecosystems frequently present A (grievance) indicators and, in some cases, I (ideological) framing; however, BAIP requires disciplined separation between (a) verifiable offender motive in the originating incident and (b) subsequent online narrative activity by third parties. Accordingly, this study treats motive assignment as conditional on verifiable sources describing observable conduct and documented intent, and it applies “Unknown/Insufficient evidence” where primary material is not available.

I (Ideología) emerged prominently in doxxing/activism hybrids, particularly where executives were framed as symbols of systemic issues (e.g., environmental, economic, or anti-corporate narratives). P (Psicopatología) appeared rarely as Primary and more often as Secondary in fixation-pattern cases, always tied to observable perseverant or disorganized contact (and, where documented, complicating factors such as substance abuse). In all instances, “P” was treated strictly as a non-diagnostic operational label.

Hybrid patterns

Multicausality was evident in 17 cases (61%). Most frequent: A+I (grievance + ideological legitimization in campaigns and escraches) and B+A (extortion layered on personal resentment). Hybrid physical-digital convergence (H1–H3) occurred in 46% of the corpus, underscoring the necessity of Digital Shield for early signal detection. Leakage and probing indicators were documented in 14 and 11 cases, respectively, often accelerating from Research/Planning to Probing stages when digital doxxing enabled physical access-seeking.

Evidence availability and constraints

U.S. cases benefited from high evidentiary quality (DOJ indictments, court filings), permitting confident pathway staging in most instances. LatAm cases relied more on aggregated official statistics and investigative reporting, resulting in Medium/Low confidence for pre-incident details in several B-dominant extortion matters. Common gaps: exact capability assessment and early grievance stage documentation. BAIP-X coding improved consistency by anchoring analysis in observable domains/families before motivational interpretation.

Table 2. Descriptive Statistics (Summary)

Metric	Value	Notes
BAIP Primary = B (Beneficio / Benefit)	9 cases	Predominantly LatAm extortion/coercion
BAIP Primary = A (Grievance)	11 cases	Predominantly U.S. grievance/insider
Hybrid frequency	17 / 28	Most common hybrids: A+I and B+A
Domain convergence (Hybrid H1–H3)	13 / 28	Digital signals enabling physical access-seeking
Most evidenced pathway stage	Research/Planning or Probing	Early stages often under-documented in LatAm sources

These patterns validate BAIP's pragmatic utility as it organizes the motivational mosaic without oversimplification, while highlighting regional differences that generic BTAM frameworks may under-emphasize.

Discussion

Implications for BTAM Applied to Executive Protection

BAIP functions as a specialized layer that strengthens BTAM's formulation phase in corporate contexts. By answering "why" through observable behavior, it focuses intelligence collection and supports proportionate mitigation. In LatAm environments, elevating B (Beneficio) reflects an operational reality—executives as efficient pressure points for instrumental gain—without departing from NTAC/DHS principles of behavioral focus and early intervention. More specifically, BAIP is innovative as a *translation layer* between BTAM and EP operations by converting motivational hypotheses into operational decisions, evidence requirements, and scalable actions—implemented through Digital Shield (DS), Protective Intelligence (PI), and GSOC AI workflows—under explicit Executive Protection Risk Management (EPRM) governance. In the retrospective corpus, motivation consistently conditioned observable patterns. B-dominant cases emphasized reconnaissance and vulnerability exploitation; A-dominant cases featured leakage and proximity-seeking; I-dominant cases involved coordinated campaigning and doxxing.

Physical-digital convergence emerges as a critical risk amplifier. In 46% of coded cases, digital signals (D2 doxxing, D1 harassment) preceded or enabled physical actions (F2 probing, H1 convergence). This reinforces the source document's insistence on Digital Shield as an essential EPRM component for detecting early indicators across BAIP categories, particularly I and hybrid A+I patterns.

Open-source reporting indicates that executive targeting has increased in volume and breadth in recent years, spanning physical attacks, protest-related targeting at predictable locations, and digital/hybrid behaviors such as impersonation, threats, swatting, and doxxing-driven convergence.[vii] These trends strengthen the practical case for EPRM integration. A digital shield functions as the early-signal and evidence-preservation layer. Protective intelligence ensures disciplined formulation and confidence

statements. GSOCs provide continuity through triage, escalation, and operational coordination. BAIP's value is clearest when it accelerates cross-functional alignment on motivation hypotheses while maintaining BTAM's core principle: decisions must be tied to observable behavior and corroborated information

Governance: Roles of Protective Intelligence and GSOC

BAIP-OP gates and RACI matrix provide defendable structure. Protective intelligence owns hypothesis formulation (BAIP-VAL), ensuring separation of facts from interpretation and explicit confidence levels. GSOC orchestrates intake, triage, alerting, and continuity, preventing analytical insights from remaining siloed. The case lifecycle (with mandatory AAR/CAPA) enables organizational learning, absent from many public records reviewed. Where organizations have adopted AI-enabled EPRM architectures, these roles can be implemented as an EPRM AI-enabled functional agent suite. A digital shield for signal detection and enrichment, PI for structured formulation and BAIP-VAL population, and GSOC for orchestration, alerting, and continuity. In this configuration, BAIP functions as a shared taxonomy to train and align both human EP practitioners and AI-enabled workflows, reducing interpretive drift while improving articulability across the case lifecycle.

Correct Use of the "P" (Psychopathology) Operational Label

The corpus reinforces the source document's caution in that "P" must remain an operational label for observable fixation/disorganization or opportunistic behavior without clear structured B/A/I drivers. It was never assigned as Primary without supporting conduct and never interpreted clinically. When justified, cases required specialist consultation (legal/mental health/LE) per proportionality principle. Misuse risks both over- and under-reaction; strict behavioral anchoring mitigates this.

LatAm Emphasis and EPRM Integration

The regional skew toward B in LatAm cases highlights why grievance-centric models alone are incomplete for EP teams operating in high-criminality environments. BAIP's integration into EPRM—Digital Shield for signals, PI for analysis, GSOC for execution—creates a closed-loop system aligned with ISO 31000 risk concepts and commonly used travel risk management practices (e.g., ISO 31030) as well as widely recognized executive protection approaches. Proportionality is preserved because it measures scale via the escalation matrix (Levels 0–4) calibrated to protectee profile, credible threats, and operational context. The validation demonstrates that BAIP improves articulability as decisions become traceable through standardized fields, reducing analyst variability and supporting governance reviews. It does not replace professional judgment but structures it, consistent with Deisinger's emphasis on operational maturity in threat management.

Limitations and Ethics

The retrospective validation presented here carries inherent methodological constraints that must be acknowledged transparently to maintain analytical integrity and support replicability. First, reliance on publicly available sources introduces documentation bias. U.S. cases benefit from detailed DOJ indictments and court filings that permit granular behavioral coding; LatAm cases more frequently appear in aggregated official statistics (e.g., extortion reports from Ecuador's National Police or Colombia's Fiscalía operations) with limited pre-incident leakage or exact pathway staging. This results in Medium/Low confidence assignments for several B-dominant cases and "Unknown / Insufficient evidence" notations for early grievance or capability indicators. The corpus therefore under-represents pure instrumental criminal cases where operational security by perpetrators limits observability.[viii]

Second, retrospective design introduces hindsight bias: post-event records may overemphasize progression once an attack or arrest occurs, while undetected or successfully mitigated cases remain invisible. The non-deterministic nature of the Pathway to Violence heuristic is respected; no claim of predictive power is made. BAIP classifies motivation on observable conduct at the time of detection; it does not forecast violence. Third, the sample size (28 cases) is modest and purposive, prioritized by LatAm-first rule and verifiability. It does not claim statistical representativeness of all executive targeting globally or regionally. Generalization is limited to patterns observable in the coded behaviors. Inter-analyst consistency was assessed internally via QA cross-check against BAIP doctrinal principles, but independent replication by third parties is encouraged using the published methodology, coding rules, and templates in the Appendices.

Ethical posture

BAIP adheres strictly to behavioral principles as analysis rests exclusively on observable, verifiable conduct. The category "P" is an operational label for patterns of persistent fixation, disorganization, or opportunistic behavior without clear structured B/A/I drivers. It is never a clinical diagnosis and does not justify inference about mental health. Specialist consultation (legal, mental health, or law enforcement) is recommended only when justified by severity, access, and proportionality. All recommendations emphasize prevention, early intervention, articulability, and risk-based proportionality calibrated to the protectee profile, credible threats, and operational context. No tactical details that could enable harm, extortion, doxxing, stalking, or attacks are disclosed. Privacy and anonymization standards are maintained; no confidential client data or internal cases are referenced. The model supports governance and defendable decision-making, consistent with ASIS EP, ISO 31000/31030, and NTAC/DHS BTAM guidelines.

Conclusion

The BAIP model offers a pragmatic, EP-specialized motivational taxonomy that addresses a documented operational gap in corporate executive protection. By organizing predominant drivers—Beneficio (instrumental criminal/economic), Agravio (perceived injustice), Ideología (symbolic/systemic attack), and Psicopatología (fixation/disorganization patterns)—into a simple, recordable framework, BAIP enables structured hypothesis formulation, targeted intelligence collection, and selection of proportional controls within the broader BTAM process and EPRM governance. Its explicit LatAm emphasis on Beneficio as a first-class category reflects regional realities of coercion and extortion without contradicting international BTAM principles of behavioral focus and early intervention.

The retrospective validation on 28 cases demonstrates that BAIP, when combined with BAIP-X behavioral taxonomy and the full operational package (BAIP-OP gates/RACI, BAIP-VAL rubric, escalation matrix, case lifecycle), improves classification clarity, recognizes hybrid patterns (especially A+I and physical-digital convergence), and supports articulable, auditable decisions. Digital Shield emerges as indispensable for capturing early signals across domains. Protective Intelligence formulates hypotheses with explicit confidence levels. GSOC orchestrates intake, alerting, and continuity. Together they close the loop from detection to proportional mitigation and organizational learning via AAR/CAPA.

BAIP does not replace professional judgment, BTAM, or EPRM. Rather, it structures them for multidisciplinary teams in high-exposure corporate environments. Its value lies in translating complex motivational mosaics into actionable intelligence while preserving strict separation of facts from interpretation and prohibiting clinical overreach. In Latin America, where instrumental criminal motives frequently predominate, this taxonomy equips protection teams to move beyond generic grievance-centric lenses toward regionally calibrated, evidence-based risk management. BAIP's contribution is

modest yet practical because it helps protection professionals think more clearly about "why" targeting occurs, so they can act more effectively, proportionally, and defensibly to safeguard executives, their families, and corporate operations.

Appendices

Appendix A: BAIP-VAL Rubric Template

Table A1. BAIP-VAL Rubric

Field	Description	Values / guidance
Case ID	Unique case identifier	Unique code
Observed conduct	Objective description of what occurred (facts only). Should include: what happened, how, when, where, and via what channel.	Structured text
Early signals	Signals detected per BAIP-X	Short list
Domain (BAIP-X)	Type of aggression	Physical / Digital / Hybrid
Behavioral family (BAIP-X)	Classification of observable behavior	F1–F5 / D1–D6 / H1–H3
Target of behavior	Actor's target	Executive / Family / Residence / Organization / Event / Physical assets / Digital assets / Reputation / Operations / Corporate
Generates concern	Concern elicited in others	Yes / No + evidence
Primary motivation (BAIP-Primary)	Dominant motivation based on evidence	B / A / I / P
Secondary motivation (BAIP-Secondary)	Secondary motivation if applicable	B / A / I / P / N-A
Confidence level	Strength of available evidence	High / Medium / Low
Actor capability	Observable capability of the actor	Low / Medium / High
Progression stage	Location on the pathway	Initial contact / Narrative / Ideation / Research / Preparation / Probing / Attack
Probable impact	Expected consequence	Low / Medium / High / Critical
Analytical interpretation	Evidence-based hypothesis	Brief narrative
Recommendation	Action suggested by Protective Intelligence	Monitor / Escalate / Mitigate / Crisis
Decision and approver	Formal resolution	Protective Program Owner (PPO) / Management / Crisis Lead
Next review	Reassessment date	Date
Associated evidence	Documentary support	Alert log / Case log / AAR / CAPA

Appendix B: BAIP-X Summary

(Physical F1–F5, Digital D1–D6, Hybrid H1–H3 with typical BAIP mapping and red flags, per EPRM).

Table A2. BAIP-X Summary (Observable Behavioral Taxonomy)

Domain	Behavioral family	Included behaviors	Early indicators	Red flags	Typical BAIP	Action
Digital approach	D1. Digital harassment and coordinated online abuse	Repeated offensive messages; smear campaigns; coordinated social attacks; hostile narrative amplification	Repeated messages; coordinated attacks; escalating language	Coordinated accounts; family targeting; prolonged persistence	A / I	Monitor + BAIP tagging
	D2. Doxxing and exposure of personal information	Publishing home address/phones/family data/routines/locations	Address publication; personal data leak; routine exposure	Calls for physical action; mass dissemination; family inclusion	I / A	Immediate escalation + mitigation
	D3. Digital extortion and reputational coercion	Threat to release information; blackmail; pressure for money or actions	Threats to disclose; money demands; blackmail	Verified information; personal references; deadlines/coercion	B	Escalate + legal coordination
	D4. Impersonation	Fake profiles; misuse of executive's name/image; deception of third parties	Fake accounts; image/name misuse; third-party outreach	Active fraud; access to contact network; corporate misuse	B / I	Containment + takedown
	D5. Unauthorized access	Account intrusion; email/social compromise; credential theft	Login alerts; password changes; suspicious access	Sustained access; exfiltration; active account use	B	Immediate response
	D6. Technical alteration or sabotage	Malware; system lockout; denial of service	System lockout; device tampering; denial of service	Operational impact; coordinated attack; persistence	B / I	Activate IT + PI
Hybrid physical–digital approach	H1. Doxxing that enables physical aggression	Publishing location with intent to harm; calling people to the home; family exposure	Publication + call-to-action; contextualized information	Calls to physically attend; route identification	I / A	Critical escalation

	H2. Device theft with intent to gain access	Targeted device theft; later use to access systems; physical→digital sequence	Suspicious loss; later account use	Coordinated attack; physical → digital sequence	B	Combined response (physical + digital)
	H3. Mobilizing third parties (swatting, hostile calls, hoaxes)	False calls to authorities; hostile mobilization; manufactured incidents	False reports; third-party activation; hostile convening	Authority intervention; media escalation	I / A	Immediate GSOC coordination
Physical approach	F1. Violent robbery oriented to access or information	Targeted assault; device theft; credential theft; access to sensitive information	Interest in laptop/phone; selective theft; subsequent account access	Correlation with digital intrusion; targeted—not opportunistic—attack	B	Immediate digital containment
	F2. Physical harassment and unauthorized approach	Stalking/following; repeated presence near the executive; unwanted contact attempts; appearances at home/work/routines	Recurrent appearances in the same locations; unsolicited interaction attempts; prolonged observation	Increased frequency; location shift (home → work); direct contact attempt	A / P	Record + monitor + identity validation
	F3. Physical surveillance, reconnaissance, and probing	Repeated observation; photo/video recording; routine identification; questions about security/access; testing team reaction	Photos/video of access points; questions about routines; presence at critical points	Systematic collection; vulnerability identification; reaction testing	B / A / I	Escalate to PI + exposure assessment
	F4. Threats and direct violence	Verbal or written threats; direct intimidation; physical assault; weapon display	Violent language; references to physical harm; explicit hostility	Specificity (place/date/method); repetition; linkage to access	A / I / B	Immediate escalation
	F5. Kidnapping	Kidnapping for ransom; express	Interest in family/asse	Vulnerability identification;	B	Preventive activation

	and physical coercion	kidnapping; unlawful restraint; coercion to obtain benefits	ts; questions about security; indirect contacts	physical tracking; actor coordination		+ law-enforcement liaison

Appendix C: Escalation Matrix (Levels 0–4)
(activation criteria, minimum actions, recipients, evidence required).
Table A3. Escalation Matrix (Levels 0–4)

Level	Operational definition	Activation criteria	Minimum action	Recipients	Required evidence
0	Isolated signal without progression	Single indicator, low confidence, no targeting	Record + monitor	PI	Initial record
1	Relevant signal without clear progression	Multiple mild indicators or persistence	Preliminary inquiry	PI + GSOC	BAIP tag + notes
2	Plausible risk	Observable progression or initial targeting	Full assessment + basic mitigation	PI + GSOC + PPO	Completed BAIP-VAL
3	High threat	Active targeting, medium/high access, multiple domains	Immediate escalation + protection plan	Management + Crisis Lead	Alerts + documented decisions
4	Imminent or ongoing threat	Advanced probing, confirmed access, clear intent	Crisis activation	Incident Command System (ICS) + all	Situation report (SITREP) + AAR

Appendix D: BAIP-OP Gates & RACI Summary
(Gates 1–6 with minimum evidence standard and responsibilities).
Table A4. BAIP-OP (RACI Summary)

Activity	R (Responsible)	A (Accountable)	C (Consulted)	I (Informed)
Intake & scoping	PI Analyst / GSOC	PI Coordinator	Legal / HR	PPO / Management
Preliminary triage	GSOC	PI Coordinator	EP Lead (EPL) / Travel / Ops	PPO
BAIP-X coding	PI Analyst	PI Coordinator	Security Risk Assessment Coordinator (SRA Coord.)	GSOC
BAIP-VAL + formulation	PI Coordinator + SRA Coord.	PPO	Legal / HR	Management
Escalation	GSOC	PPO	ICS / Crisis Lead	Stakeholders
Case management & closure	PI Coordinator	PPO	Audit / QA	Management

Appendix E: Simplified BAIP–Pathway to Violence Mapping Table
(reproduced from EPRM).

Table A5. Pathway to Violence Matrix Mapped to BAIP (Simplified)

Pathway stage	Observable behavior for B (Benefit)	Observable behavior for A (Grievance)	Observable behavior for I (Ideology)	Observable behavior for P (Psychopathology – operational label)
1. Grievance / trigger	Instrumental interest in money/assets/PII of the protectee. **Management:** elevate exposure hygiene; validate coercion indicators.	Persistent injustice narrative; victimization. **Management:** control contact points; activate HR/Legal if applicable.	Cause-based language; executive framed as a "symbol." **Management:** monitor campaigns/communities; map triggering events.	Early fixation without coherent grievance; strange contact. **Management:** document and set contact boundaries early.
2. Ideation	Threats/blackmail (implicit or explicit) oriented to obtaining something. **Management:** triage gate → PI; prepare LE liaison per threshold.	Leakage of punishment; fantasies of "making them pay." **Management:** elevate concern; prioritize access/proximity in BAIP-VAL.	Moral justification of harm; glorification/copycat framing. **Management:** reinforce event security; evaluate mobilization.	Idiosyncratic/incoherent/delusional ideation; perseverance. **Management:** do not diagnose; escalate specialist consult per severity.
3. Research & planning	Physical/digital reconnaissance; searching for vulnerabilities. **Management:** elevate to Full Assessment if targeting is verifiable.	Research on the executive (routines, residence, family). **Management:** reduce exposure; evaluate means/capability.	Planning for protests/harassment; preparatory doxxing. **Management:** coordinate with GSOC; home/event scenarios.	Repetitive/obsessive information seeking; erratic patterns. **Management:** contact rules + exhaustive documentation.
4. Preparation	Acquisition of means; secondary surveillance; logistics. **Management:** harden routes/residence; crisis coordination.	Escalating frequency; more direct contact attempts. **Management:** increase access control and protection measures.	Coordination of third parties; convening; testing response. **Management:** raise event thresholds; prepare tactical response.	Disorganized conduct exploiting opportunity; repeated approaches. **Management:** clear limits + LE/subject-matter expert (SME) consult if access increases.
5. Probing & breaching	Security probing; approaches; validating access.	Presence at critical points; physical contact; intrusion.	Doxxing with call for physical action; swatting/hoax.	Repeated intrusions; stalking-like;

	Management: critical escalation (imminent threat) + plan.	**Management:** intensive protection; consider legal orders/actions.	**Management:** immediate GSOC coordination; harden home/event.	unpredictability. **Management:** rapid response + documentation; prioritize physical safety.
6. Attack / implementation	Attempted kidnapping/coercion/directed assault. **Management:** activate crisis + LE; preserve evidence.	Direct assault; attack on symbolic grievance target. **Management:** crisis + post-incident AAR/CAPA.	Attack at event/home; amplified/propagandistic action. **Management:** crisis + reputational/continuity coordination.	Opportunistic violence enabled by access/exposure. **Management:** immediate response + review protection failures.

Author: Kevin E. Palacios is CEO of HELPS Latam, a Quito-based firm delivering protective services, secure transportation, and protective intelligence across 18 countries in Latin America. With more than 25 years of operational experience leading executive protection details in high-threat environments, he specializes in translating protective intelligence into actionable risk mitigation strategies.

Endnotes

[i] National Threat Assessment Center, *Behavioral Threat Assessment Units: A Guide for State and Local Law Enforcement to Prevent Targeted Violence* (Washington, DC: U.S. Secret Service, 2024).
[ii] Security Executive Council, *Executive Targeting Report: Analysis of Attacks on Corporate Executives from 2003–2025* (Ann Arbor, MI: Security Executive Council, 2026), https://securityexecutivecouncil.com/insight/program-best-practices/executive-targeting-report-analysis-of-attacks-on-corporate-executives-from-2003-2025-2615 (accessed April 22, 2026).
[iii] Kevin Palacios, *Volume I: Executive Protection Manager – EPM: Handbook on Strategic Protection Management from a Risk Perspective (EPRM: Executive Protection Risk Management 1)* (Amazon Kindle, 2024); Kevin Palacios, *Leveraging Artificial Intelligence to Enhance Executive Protection Risk Management (EPRM)*, *Close Protection Security Journal* (CPSJ) 3, no. 1 (July 1, 2025).
[iv] Ibid.
[v] Frederick S. Calhoun and Stephen W. Weston, *Contemporary Threat Management: A Practical Guide for Identifying, Assessing, and Managing Individuals of Violent Intent* (Alachua, FL: Specialized Training Services, 2003); Cybersecurity and Infrastructure Security Agency, "Pathway to Violence: Warning Signs and What You Can Do," 2023, https://www.cisa.gov/resources-tools/resources/pathway-violence (accessed April 22, 2026).
[vi] U.S. Department of Justice, "Final Defendant in eBay Cyberstalking Case Sentenced," July 18, 2024, https://www.justice.gov/usao-ma/pr/final-defendant-ebay-cyberstalking-case-sentenced (accessed April 22, 2026); U.S. Department of Justice, "eBay Inc. to Pay $3 Million in Connection with Corporate Cyberstalking Campaign," January 11, 2024, https://www.justice.gov/opa/pr/ebay-inc-pay-3-million-connection-corporate-cyberstalking-campaign (accessed April 22, 2026).

[vii] Aaron Katersky et al., "Executive 'Hit Lists' and Wanted Posters: NYPD Warns about Threats to Executives," *ABC News*, December 11, 2024; TAL Global, "The Contagion Effect: What The UnitedHealthcare CEO's Assassination Means for C-Suite Security," December 17, 2024.
[viii] Aggregated prosecutorial and law enforcement reporting on extortion/coercion operations in Colombia and Ecuador (2024–2025), used for contextual frequency and typology only where pre-incident behavioral detail was not publicly available.

Selected key sources

- Calhoun, Frederick S., and Stephen W. Weston. *Contemporary Threat Management: A Practical Guide for Identifying, Assessing, and Managing Individuals of Violent Intent*. Specialized Training Services, 2003.
- Corner, Emily, et al. "Grievance-Fuelled Violence: Modelling the Process of Grievance Development." Australian Institute of Criminology Research Report No. 27, 2023.
- National Threat Assessment Center. *Behavioral Threat Assessment Units: A Guide for State and Local Law Enforcement to Prevent Targeted Violence*. U.S. Secret Service, 2024.
- U.S. Department of Homeland Security, Center for Prevention Programs and Partnerships (CP3). *Behavioral Threat Assessment and Management in Practice*. 2024.
- Security Executive Council. *Executive Targeting Report: Analysis of Attacks on Corporate Executives from 2003–2025*. 2026.
- U.S. Department of Justice. "eBay Inc. to Pay $3 Million in Connection with Corporate Cyberstalking Campaign Targeting." January 11, 2024.
- Additional sources for corpus cases: official Fiscalía reports on extortion operations in Colombia/Ecuador/Mexico; court records on insider threats; NTAC/DHS-aligned materials; ASIS benchmarking reports. All claims tied to verifiable primaries or aggregated official statistics where granular detail is limited.

Professional Articles

Technical Surveillance Countermeasures: A Risk-Based Approach to Protecting Sensitive Information

Chuck Tobin and Jordan Kelly

Why Sensitive Conversations Are at Risk

Business confidential information is frequently targeted by a range of adversaries for political and commercial espionage purposes. The Federal Bureau of Investigation (FBI) estimates that espionage costs the American economy hundreds of billions of dollars annually, with adversaries targeting sensitive information across the defense, intelligence, economic, financial, public health, science and technology sectors.[i] These adversaries include nation states conducting intelligence operations for political advantage, corporations seeking competitive advantage during negotiations, bids, or disputes, criminals motivated by financial gain, and malicious individuals acting out of personal grievance. The distinction between state actors and competing foreign corporations is often blurred, as authoritarian states may compel private companies to conduct intelligence operations on their behalf for political and economic gain.[ii]

Sensitive information of strategic value is commonly discussed in boardrooms and executive offices, environments that adversaries actively seek to exploit. However, these discussions also frequently occur in less controlled settings: executive residences, vehicles, hotels, and other external venues. This shift has increased the attack surface, exposing these conversations to a range of collection methods. These include eavesdropping devices that transmit information using a variety of technologies, ranging from requiring someone to be within range of a space to receive the information, to completely remote collection using cellular or Wi-Fi networks. Devices without the capability to transmit and store data locally are placed and retrieved at a later stage, requiring the adversary to access the target space on two separate occasions. Wireless information security threats present an additional vector, including malicious Wi-Fi access points that intercept data when an executive connects to what appears to be a legitimate network, and IMSI catchers, portable devices that mimic a cell tower and trick a targeted mobile device into connecting and exposing its communications.[iii] Unsecured technology within a space that contains a microphone or camera can also be exploited to capture sensitive conversations and footage.

The true scale of this threat remains unknown, as many organizations may choose not to disclose incidents due to concerns around reputational damage, legal exposure, or commercial sensitivity.[iv] Many cases are also likely undetected or are only discovered after intelligence collection has already taken place. For example, in 2024, multiple eavesdropping devices were detected inside the offices of a luxury Italian yacht manufacturer during a shareholder dispute involving a Chinese state-linked entity. The devices were only identified after an executive became suspicious of being under technical surveillance and commissioned a TSCM inspection.[v] Technical Surveillance Counter-Measures (TSCM) is an on-the-ground inspection of sensitive spaces conducted by specialist operators using advanced equipment to detect and mitigate eavesdropping devices, wireless threats, and associated vulnerabilities. TSCM can be conducted across a range of environments, from offices and residences to vehicles. For an inspection to be impactful, it is important to consider whether access to the space can be effectively controlled to maintain the integrity of the inspections.

What a Risk-Based Assessment for TSCM Looks Like

Despite this being an increasing and widespread risk, the commissioning of a TSCM inspection has traditionally tended to be reactive, applied inconsistently, or initiated only after intelligence collection has already taken place.[vi] A proactive, intelligence-driven approach can address these gaps by aligning the deployment of TSCM to identified risks. Established risk assessment frameworks within the executive protection discipline direct that security measures should be deployed on the basis of threat, vulnerability, likelihood and consequence.[vii] Applying this approach to TSCM allows inspection decisions to be grounded in assessed risk rather than instinct. Within this model, specific events or activities may trigger a risk assessment to determine whether an inspection is warranted. Such triggers can include mergers and acquisitions or competitive bidding activity, commercial or private litigation matters, the purchase of a new executive asset including a residence or aircraft, executive travel, relocation to a new office space or following periods of construction, and highly sensitive executive meetings. Each of these circumstances can involve the discussion of sensitive information beyond day-to-day business operations. Internal teams supporting executives are likely already tracking many of these events as part of a wider protective program, making them a natural and consistent entry point to the assessment process. Partnerships with the Insider Threat program, Workplace Violence Prevention Program, General Counsel's Office, and Risk Management will greatly advance the programs insights into the threat vectors that face the organization.

An executive protection risk assessment broadly examines the threat actors present in a specific location, their precedence of targeting, likelihood of activity, and potential impact to determine proportionate precautions. In the context of TSCM, several considerations may inform whether an inspection is a proportionate response. The first is whether threat actors with the motive, capability, and opportunity to target the organization are likely to be operating in the location where the event or activity is occurring. Certain cities or jurisdictions present a higher concentration of adversaries due to the presence of attractive targets such as political institutions, financial centers, or organizations with significant intellectual property, and a meeting held in such an environment may carry a materially higher risk of information theft. The specific venue may also warrant consideration, particularly where a threat actor has a direct line of sight into the space or access to shared infrastructure. The next consideration is consequence severity: the operational, financial, reputational, or legal cost if that conversation were compromised. A negotiation strategy reaching a counterparty, a litigation position being exposed, or a board discussion becoming public can each carry significant consequences. Additional factors may also be relevant, including an executive's risk profile or activities that heighten personal exposure to targeting. Contemporary concerns include a heightened risk of the installation of concealed cameras at rental properties, restrooms, and locker rooms.[viii] The ease of acquisition of these devices elevates significant concerns around the publication of intimate photos of executives. Considered together, these factors provide a basis for determining whether TSCM is a proportionate form of risk mitigation, with the appropriate threshold informed by the organization's appetite for risk.

This framework supports decision-making that is documented, traceable, and aligned to identified risks. A structured assessment produces a rationale that goes beyond the event or activity itself, capturing the specific threat actors and risk factors considered, rather than an inspection simply being associated with a particular event. This approach reflects the broader shift across the executive protection industry, where security services are increasingly commissioned on the basis of structured risk assessment rather than instinct.

One-Off or Programmatic: Determining the Right Approach

TSCM services are often spontaneous and associated with new exposures such as new executive travel; or related to a newly identified concern. The One-Off approach is essential in supporting the ongoing and constantly changing environments an executive travels through. The hotel rooms, cars, aircraft, conference rooms, and vessels they utilize are often not owned assets, but represent a temporary venue that creates an unknown risk and potential exposure. Within the construct of an executive protection programs TSCM efforts, they must consider how they will support these constantly changing requirements. These requirements, often spontaneous, require a highly flexible TSCM partnership. Depending upon the risk assessed during the aforementioned risk assessment process, the executive protection program may require sweeps of the various locations globally and sometimes on very short notice.

Foundationally, however, an executive protection program must establish a programmatic approach to TSCM sweeps and countermeasures. This should be part of an organizations Enterprise Security Risk Management (ESRM) security policy. The programmatic approach ensures that a baseline is set and less dependency is placed upon spontaneous concerns, which as noted earlier are requested after the concern for loss of information is identified. A programmatic approach sets thresholds for the depth of TSCM services required, frequency of reinspection, and a delivery model.

A programmatic approach relies upon the risk modeling to build program requirements. The types of threats assessed during the risk assessment process greatly influence this model. Nation state actors vs. insider threats different concerns to the program. The nation state actor may have access to complex technologies inaccessible to the insider. Insiders themselves may include persons bearing a grudge against the leadership, such as someone subject to an impending reduction in force decision; to someone acting on behalf of an external entity such as a corporation, state actors, or criminal enterprise. The perceived capabilities of the actor directly influence the level of effort and technologies required by the program.

The depth of services required does not just include the technologies utilized, but the manner in which they are utilized. The beneficiary of the sweep likely has predetermined expectations regarding the results of the sweep. Their assumption suggests that from the point the sweep is performed and beyond, their conversations are protected. The reality is that the second the sweep is concluded that protection goes away unless security controls are put in place. An element of the programmatic approach is to secure the security of the inspected space post inspection. Restricting the access of new and unscreened technologies such as cell phones, is essential to ensuring this base line. Absent a sophisticated and mature TSCM program, these types of vulnerabilities will eventually diminish the efforts of a program. Bluetooth devices, Wi-Fi-enabled devices, cell phones, laptops, etc. all may come and go through a protected workspace. The program must establish strict security protocols to extend the life of a TSCM sweep.

In certain circumstances, the programs risk assessment may suggest in-place detection efforts are necessary.[ix] Events such as board meetings or other highly sensitive meetings may require active surveillance by technicians throughout the course of the meeting. Both models, the One-Off and Programmatic approach are essential to a comprehensive TSCM program. A proper program will set the base requirements and limit unknown conditions that could create exposure. This program will also best define when to procure spontaneous support, diminishing fear-based service engagements and more importantly, mitigating the requirement to sweep after a threat has been presented.

The Benefits of an Intelligence-Driven, Risk-Based Approach

At this point, the benefits of a risk-based approach should be clear. The risk-based approach to TSCM aligns itself with the enterprise risks that are present for shareholders and key stakeholders. It doesn't sweep for the sake of sweeping, it sweeps to proactively eliminate the unknown. It doesn't respond unnecessarily to threats, it works to eliminate the baseline risks through security policy and controls while responding to the spontaneous elevated concern. Through coordinated efforts the program has gained insights into the threats facing the organization. In contemplating the capabilities and likelihood of those threats, the program evaluates the vulnerabilities that may further increase the risk of exploitation of sensitive information. They then, put countermeasures in place. Countermeasures that detect & identify devices and potentially the actors behind them.

An intelligence-driven model also pulls the TSCM program out of the dark. TSCM is often misunderstood by security leaders and as a result, difficult for them to defend or even present to key leaders as a risk they need to mitigate. In a holistic protection model, established by the executive protection program, TSCM services are part of the norm. Just like Digital Executive Protection (DEP) and concerns raised by the compromise of digital information; the TSCM program is a key component of information security in executive protection. As a part of the broader information security mission, the TSCM program authors should work closely with persons responsible for limiting access to executive calendars and sensitive information, event organizers and legal partners that may print and later dispose of printed confidential information; and cyber security partners that protect devices in-place and in-transit.

In summary, program managers must first invest in the risk assessment process. Risk assessments that set an organizational baseline and inform security policy. Also, they must prepare for event-based risk assessments that respond to changing conditions in an executive's environment. The culmination of this effort results in a comprehensive intelligence-driven TSCM program that provides for the ongoing programmatic assessment requirements of office spaces, vehicles, aircraft, and residences; while also navigating the constantly changing horizon of executive travel. Travel to temporary lodging, meeting spaces, vehicles, aircraft, and vessels.

Authors:

Chuck Tobin is the President and CEO of AT-RISK International since 2003, bringing over 35 years of experience protecting people, property, and operations for clients worldwide. Tobin has provided protective services across the globe and served as National Director of Security and consultant to the United States Presidential, Prime Minister, and international elected official campaigns around the world. He is also the President of IPSB, the Chair of Standards and Guidelines on the ASIS Executive Protection Council, and from 2013 to 2017, Mr. Tobin acted as President of the Association of Threat Assessment Professionals.

Jordan Kelly is co-founder and director of Proactive Privacy, a London-based executive risk management and Technical Surveillance Countermeasures consultancy that supports clients globally. He served nine years in the British Army with the Parachute Regiment, including four years within the Special Forces Support Group with an operational deployment conducting counter-terrorism duties. Following his military service, Jordan held a specialist security roles in technology companies and for high-net worth individuals.

Endnotes

[i] Federal Bureau of Investigation, "Counterintelligence," FBI.gov, https://www.fbi.gov/investigate/counterintelligence.
[ii] National Protective Security Authority, "Secure Innovation: Company Guidance," NPSA.gov.uk, https://www.npsa.gov.uk/specialised-guidance/secure-innovation/company-guidance.
[iii] National Institute of Standards and Technology, "Bolstering Data Privacy and Mobile Security: An Assessment of IMSI Catcher Threats," NIST.gov, https://www.nist.gov/speech-testimony/bolstering-data-privacy-and-mobile-security-assessment-imsi-catcher-threats.
[iv] Federal Bureau of Investigation, "Combating Economic Espionage and Trade Secret Theft," FBI.gov, https://www.fbi.gov/news/speeches-and-testimony/combating-economic-espionage-and-trade-secret-theft.
[v] Bloomberg News, "Italy-Based Luxury Yacht Maker Ferretti Faces Spying Claims," *Bloomberg*, June 6, 2025, https://www.bloomberg.com/news/articles/2025-06-06/italy-based-luxury-yacht-maker-ferretti-faces-spying-claims.
[vi] Bastille Networks, "Technical Surveillance Countermeasures," Bastille.net, https://bastille.net/centers-of-excellence/tscm/.
[vii] Joe M. Olivarez Jr., "ASIS International Introduces Groundbreaking Executive Protection Standard," ASIS International, September 23, 2025, https://www.asisonline.org/security-news/press-room/asis-international-introduces-groundbreaking-executive-protection-standard/.
[viii] Airbnb Says Hidden Cameras Are Banned. Here Is What Actually Happens When Guests Find One. (March 27, 2026). StaySTRA.com. https://staystra.com/airbnb-hidden-camera-policy-enforcement-2026/.
[ix] *United States Department of Defense, "Technical Surveillance Countermeasures (TSCM)"*. 2014. Washington, DC. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/524005_2014.pdf.

Protective Medicine: The Interface of Concierge Medicine, Executive Health, and Executive Protection

Robert L. Quigley, MD, DPhil

Abstract

December 4, 2024 is a day that will always be remembered in so many international communities. This day at 0644 hours Brian Thompson, the CEO of United Healthcare, was assassinated in midtown Manhattan, New York, on his way to the annual UnitedHealth Group investors meeting. Reactions to his untimely death varied. In the insurance space many competing providers swiftly reversed any of their (controversial) policies in an effort to steer attention away from the industry which for so long has been scrutinized for denial of benefits and excess profits.[i] In the Executive Protection community, whether employed by an ultra-high-net-worth Principal, a Family Office, or a Corporation, any and all services were completely overhauled. The number of agents on any detail was immediately ramped up as was their training in first aid (ironically Mr. Thompson had no security accompanying him at the time of his death).[ii] In the process of the aforementioned (unsustainable) "overhaul" the requisite due diligence performed by EP leaders revealed that the greatest exposure for their protectee(s) is not an assassination but rather an adverse health incident. This paper serves to justify the purpose and value of including protective medicine leadership/input on any/all EP services. Today, such inclusion not only represents a duty of care responsibility but best practice.

Introduction

Most executive protection (EP) services operate under the governance of a structured actionable framework referred to as a crisis management plan (CMP). Part of the plan includes the identification of risks, the assignment of roles and responsibilities, the confirmation of communication strategies, and ultimately response procedures. The CMP typically outlines a roadmap for personal security, physical infrastructure, and hardware and software (cyber). Often overlooked is the enterprise health plan (EHP). This (EHP) vertical within the CMP should include procedures to manage any illness or injury (ideally based on the medical risks specific to the Principal and ALL those covered) but also an infectious disease plan (particularly with travel to disease endemic nations), a pandemic plan (COVID-19 was a disaster for so many unprepared EP services), and finally a chemical, biological, radioactive, and nuclear (CBRN) plan. The enterprise health plan should also include one for mental illness (potentially impacting not just the principal but their family, their companions, and even fellow agents).

In 2025, according to Esgauge, a data analytics firm, 43% of top bosses (CEOs/Principals) are in their fifties, while 42% are at least 60 and only 15% are younger than 50 years. Similarly, recent health data reveals the chronic disease burden in those over 50 years of age is extremely high with over 75%-85% affected with at least one condition and some dealing with multi-morbidities. Cardiovascular diseases (inclusive of hypertension**,** heart attack and stroke), diabetes, and obesity are the most common non-communicable diseases (NCDs) impacting their lives.[iii] In addition, 50% of the world's population will develop a mental

health disorder at some point in their lifetime.[iv] No one is immune from developing these aforementioned physical or mental conditions, particularly the global business leaders of today. Unfortunately, many impacted are either in complete denial of their health risks or unwilling to share such personal health information (PHI) even in the context of HIPAA or GDPR laws. Some are concerned that disclosure of any PHI would reveal vulnerability and even threaten their job security. This latter reality only adds another layer of complexity for medical professionals tasked with maintaining the health and welfare of their principal(s).

Protective Medicine

Protective Medicine (PM) has evolved into a medical sub-specialty that focuses on the prevention, recognition, and management of illness, injury, and the identification of health risks in individuals under protective security. Visually, PM can be best represented by the Venn diagram in Figure I below.

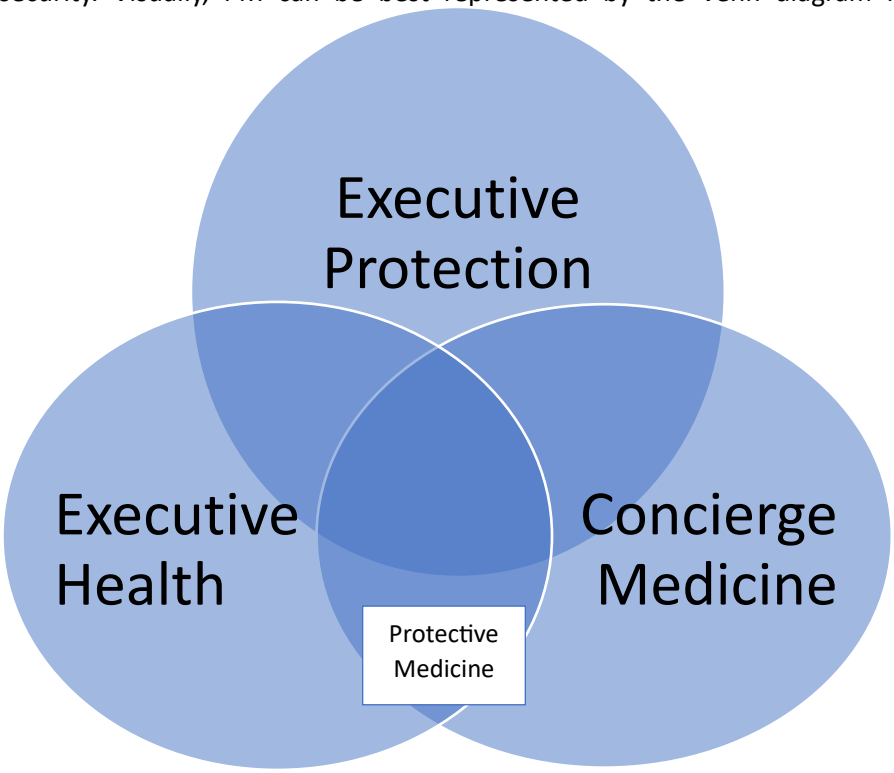

Figure I: Protective Medicine represents the interface of executive health, concierge medicine, and executive protection

The PM sub-specialist, with the appropriate pedigree, can and should enhance and complement any EP service. Five non-negotiable pre-requisites for the role include: expertise in emergency, trauma or critical care, global experience and familiarity with multiple healthcare systems, an unrestricted medical license, 24/7 availability with surge capacity with ability to determine fitness-to-fly, choreography of a medical evacuation (bed-bed) while maintaining working relationships with any or all global medical assistance companies, and discrete professional behaviors guided by HIPAA/GDPR laws beyond the Hippocratic oath.

There are multiple business models designed to incorporate a PM sub-specialist on the EP team. The doctor can operate as a fulltime equivalent or a fractional medical director. He or she can function independently or as a point of escalation for emergency medical service professionals working in the field

(i.e., EMTs and RNs) applying the details of the specific medical emergency response plan (MERP). He or she can even perform in both capacities depending on the time, location, and need(s) of the principal.

Other merits of the doctor that are ideal but not mandatory include experience in aviation or maritime medicine, ability and credibility to work collaboratively with existing primary care providers (not to replace their services but rather to enhance them), capable of securing (bespoke) medical equipment (inclusive of first aid kits and AEDs, qualified (global) medical escorts, and medicines (prescription and non-prescription)), access to a (global) stable of doctors (for house calls and local prescriptions), and finally knowledge in the design and implementation of medical emergency response plans (MERPs).

The MERP

The MERP is a dynamic document created for the principal, and anyone else for whom the EP team is responsible. It is a collaboration between the PM sub-specialist and the chief security officer (CSO). It is considered best practice to create a new one for any and all activities at home, during travel (whether that is terrestrial, maritime or aviation), and at any event (house party or otherwise). The contents should be based on an initial risk assessment for sickness and injury (destination- and activity-specific) but should also contain a plan to address any psychological incident affecting the principal, his or her companions, and family (even fellow agents). Principals may be on psychotropic drugs to manage anxiety, depression, stress or insomnia. Their children may have behavioral disorders (treated or untreated). Companions, while in their company, may be using illegal drugs.

The MERP should follow a standard template to include (at least) the following elements: a project risk register used to identify, analyze, and track potential risks usually created on a spreadsheet and shared with ALL; commitment by ALL members of the team to review (following a schedule), and regularly update, a communication protocol that includes a list of all stakeholders, their contact details, and their respective role(s) in the event of an emergency; evacuation and emergency mission-specific procedures outlining evacuation routes and modes of mobilization for multiple scenarios inclusive of severe weather, fire, and adverse medical incidents (i.e., site emergency response); identification of triage and final hospital care (in the event care needs upgrade and sick or injured patient is determined fit-to-fly by PM sub-specialist (a psychiatric facility should also be included in this element)); a team-approved list of terrestrial and aviation transport providers; diplomatic resources and contact details (for assistance with any immigration or passport issues); currency access in the event (medical) fee-for-service(s) requires cash payment(s); details of bespoke medical equipment and personnel that may be required for the mission; and finally specific principal personal health information (PHI) and that of anyone else under protection, such as existing chronic disease(s), prescribed (with a copy of the Rx) and non-prescribed medicines, allergies, etc.[v] Occasionally, this PHI is kept under separate cover and only revealed by the PM sub-specialist if or when critically necessary.

Additional Job Description for the PM Sub-Specialist

Besides co-ownership of the MERP (with the CSO), the PM sub-specialist has multiple other responsibilities including but not limited to the ability to provide medical kits (including AEDs) at residence(s) and in the transportation vehicles (plane, car, yacht). The kits should also contain any medicines relevant to the needs of the Principal as well as resuscitative medicines like Epinephrine and Naloxone for allergic reactions and narcotic overdose respectively along with the time and place to train house managers, staff, and EP personnel on basics in First Aid, use of an AED, and “stop the bleed” (it is important to recognize that staff are often not comfortable touching the principal or their guests so creative solutions are required if they are to assume the role of first responders). The PM sub-specialist should provide the AEDs, as well as any

service contract, and the qualified trainers for the HM and staff (he or she should also keep records on who has been trained and when they were trained). They should outfit every residence with a medical alert system, whether mobile or stationary where the staff or principal can access it 24/7 in an emergency response center to activate the MERP and simultaneously notify the CSO/MD.

Relatedly, they need to ensure that (laminated) emergency contact numbers are placed on walls throughout the residence(s) next to a landline (if one exists) or in central locations within the residence (i.e., kitchen, family room, pool deck, etc.). It is noteworthy that different emergency numbers exist depending on location. In the United States, it is 911. The equivalent in the UK is 999, in the EU it is 112, and in Australia it is 000 or 112 (when using mobile phone). Finally, they need to implement miscellaneous health and safety considerations, particularly where underlying musculoskeletal issues impact occupants, and ensure the installation of smoke and carbon monoxide sensors in all residences, ideally checked bi-annually.

Duty of Care

Duty of care has legal, ethical commercial, fiduciary and social responsibility applications but there are unique applications in the workplace and corporate contexts. Specifically in the workplace, duty of care means the development of policies and procedures to mitigate against "foreseeable" risks. In most jurisdictions failure to do so is managed by the courts as a civil infraction. However, in Canada and the UK such failure is prosecuted as a criminal offence. In Canada the Westray bill (Bill c-45) was passed by Parliament in 2003, and in the UK the Corporate Manslaughter and Corporate Homicide law was passed by Parliament in 2007.[vi,vii] Both laws are enforced against any organization that does not meet their duty of care by not having and enforcing policies and procedures to mitigate against "foreseeable" risks. In Canada, the bill was further modified (section 217.1) such that any individual with responsibility over another can be held criminally liable if they do not meet their duty of care responsibilities regarding "foreseeable" risks.

Unfortunately, many incidents in the field encountered by the EP team are "foreseeable," particularly medical ones. For example, it is a "foreseeable" risk that the principal (and anyone in his or her company) could suffer a cardiovascular event (i.e., stroke or heart attack), food poisoning, heat stroke, etc. If there are not memorialized policies and procedures in place, then the CSO could be held responsible for not meeting his or her duty of care or for not having a medical expert on the EP team with expertise and protocols to manage such an adverse health event.

Conclusion

In 1985, two renowned experts in leadership coined the acronym VUCA (Volatility, Uncertainty, Complexity, and Ambiguity) in their classic management book *Leaders-Strategies for Taking Charge*.[viii] At the time the acronym represented the conditions organizations faced when making decisions and mitigating risks. These same four elements have historically been used in the EP space as a conceptual tool that underscores the challenges confronted when agents strive to meet their duty of care.

The world, however, has evolved and transformed and the VUCA model no longer captures the disruptions and chaos that prevail today and thus has been largely replaced by a more applicable model coined by the futurist Jamais Cascio in 2018: BANI (Brittle, Anxious, Non-Linear, and Incomprehensible).[ix] The EP provider of today must incorporate this taxonomy of chaos into their daily operations to best support their principals. To succeed, a brittle system needs resilience, an anxiety fueled system needs empathy, a nonlinear system needs improvisation, and an incomprehensible system needs intuition.

EP professionals are trained to follow structure, and BANI helps compartmentalize the ubiquitous chaos under which we all operate. In that same spirit, EP professionals support metrics and key performance indices (KPI's). Unfortunately, the BANI responses to chaos (resilience, empathy, improvisation, and intuition) are difficult to quantify. To that end, and looking to the future, the profession must continue to adapt through introspection and curiosity. In these uncertain times, existing services no longer meet the holistic needs of the clients. Inclusion of a medical expert on the EP team will simply enhance their value proposition and in so doing meet any duty of care requirements. This is best practice.

Author: Robert L. Quigley is the owner of RLQ LLC a global protective medicine service exclusively serving UHNW/FOs. He previously served as a Global Medical Director/SVP at International SOS Assistance. Prior to that he was a Professor of Cardiac & Trauma surgery. He is a prolific author, a KOL, and a subject matter expert in duty of care. He has been invited to speak at multiple global security forums including ASIS International, ISMA, ESOC, RIMS, and Inside NGO.

Endnotes

[i] M. J. Alkire, S. Saha, and M. Ingram, "Trend Alert: Private Payers Retain Profits by Refusing or Delaying Legitimate Medical Claims," *Premier Inc.*, March 21, 2024, https://www.premierinc.com.
[ii] M. Gates, "How Executive Protection Is Changing One Year After UnitedHealthcare CEO Attack," *Security Management* (ASIS International), December 4, 2025.
[iii] K. B. Watson, J. L. Wiltz, K. Nhim, et al., "Trends in Multiple Chronic Conditions Among US Adults, by Life Stage, Behavioral Risk Factor Surveillance System, 2013–2023," *Preventing Chronic Disease* 22 (2025): 240539, https://doi.org/10.5888/pcd22.240539.
[iv] Ronald C. Kessler, Matthias Angermeyer, James C. Anthony, et al., "Lifetime Prevalence and Age-of-Onset Distributions of Mental Disorders in the World Health Organization's World Mental Health Survey Initiative," *World Psychiatry* 6, no. 3 (October 2007): 168–176.
[v] Occupational Safety and Health Administration, "Fire, Rescue, and Medical Services," *ETool: Evacuation Plans and Procedures – Emergency Action Plan*, accessed June 22, 2026, https://www.osha.gov/etools/evacuation-plans-procedures/eap/fire-rescue-medical.
[vi] Canadian Centre for Occupational Health and Safety, "Westray Bill (Bill C-45) – Overview," *OSH Answers*, December 10, 2020, https://www.ccohs.ca/oshanswers/legisl/billc45.html.
[vii] United Kingdom, "Corporate Manslaughter and Corporate Homicide Act 2007," *legislation.gov.uk*, 2007, https://www.legislation.gov.uk/ukpga/2007/19/contents.
[viii] Warren Bennis and Burt Nanus, *Leaders: Strategies for Taking Charge* (New York: Harper & Row, 1985).
[ix] Jamais Cascio, "Human Responses to a BANI World," *Medium*, October 21, 2022, https://medium.com/@cascio/human-resources-to-a-bani-world-fb3a296e9cac.

The Unsettled States of America: The Normalization of Violence, the Evolution of Vigilantism, and Soft-Target Violence

Matthew E. Nieminski

Introduction: The Quiet Reclassification of Violence

For much of modern American history, political violence occupied the "fringe" margins of society, appearing as a disruption rather than a condition. Acts of violence were something that erupted, briefly and tragically, before receding again into the realm of the exceptional and unexpected. The dominant assumption, embedded in both public discourse and institutional planning, was that such acts were aberrations carried out by isolated individuals or extremist enclaves.[i] Recently, however, that assumption appears increasingly strained. A pattern of incidents, targeted attacks on public officials,[ii] violence directed at religious institutions, [iii] and ideologically ambiguous assaults on symbolic spaces, [iv] suggests a reclassification. Violence is no longer consistently interpreted as extraordinary. Instead, it is being absorbed into the ambient understanding of risk that shapes daily life. [v] This shift is subtle but consequential. When violence moves from exception to expectation, it alters not only how societies respond, but how they perceive themselves.

The Digital Theater of Violence

If violence and violent acts have become more visible, it is in no small part because it has become more *circulated*. The modern information environment recycles, reframes, and redistributes them. Digital platforms and social media transform acts of violence into persistent artifacts, clips, narratives, and symbols that outlive the incidents themselves.[vi] Algorithmic amplification plays a decisive role. Content that provokes outrage, fear, or fascination is elevated and promoted, ensuring that violent acts receive disproportionate attention relative to their statistical frequency.[vii] Over time, this creates a perceptual distortion: violence appears not only more common, but more central.[viii]

The rise and increasing popularity of "true crime" as a dominant cultural genre further complicates this dynamic. While often framed as analytical or documentary and intended to inform or analyze, such content may intentionally or unintentionally frame violence in ways that emphasize and at times even fetishize intrigue or personality, rather than consequence. Recent "documentaries" focused on Aaron Hernandez, Ed Gein, John Wayne Gacy, Jeffrey Dahmer, and the Menendez Brothers shine an arguably over sympathetic light on the perpetrators.[ix] In some cases, this contributes to the normalization of violent behavior.[x] Perpetrators become characters; motives become story arcs. In this translation from event to narrative, consequence and heinous action is often overshadowed by intrigue and an attempt to sympathize and to understand.[xi] The result is what scholars have described as a form of mediated notoriety, in which visibility itself becomes a reward structure.[xii] For certain individuals, particularly those operating at the margins, visibility in today's "attention economy" may function as incentive. Consequently, alleged murders, such as Luigi Mangione and Tyler Robinson could become semi-mythological folk "heroes" in some circles and digital information silos.

Vigilantism Without Structure

Parallel to these developments is the evolution of vigilantism. Historically, vigilantism emerged in localized contexts, often as a response to perceived gaps in formal law enforcement. Today, it has been unbound from geography. Contemporary vigilantism is decentralized, digitally mediated, and ideologically fluid. Participants are not organized in traditional organized criminal or terrorist hierarchies; they are merely connected through narratives, shared grievances, conspiratorial frameworks, or political identities that transcend physical proximity.[xiii] This transformation has profound implications. Without formal structure, there is little to disrupt. Without leadership, there is no clear point of intervention. Action emerges from convergence: individuals arriving at similar conclusions through shared informational ecosystems.[xiv] In such an environment, legitimacy is often self-assigned. Actors frame their behavior as corrective or protective, justified by perceived institutional failure.[xv] The result is a form of violence that is both individualized and collectively reinforced, a paradox that complicates both prediction and prevention.

The Erosion of Civic Space

As violence becomes more normalized, its effects extend beyond immediate harm. It reshapes the meaning of public space. Schools, houses of worship, and community venues, once defined by a welcoming openness, are increasingly viewed through a lens of risk and vulnerability.[xvi] This perceptual shift carries operational consequences. Security measures that were once out of the ordinary have become routine: controlled access points, surveillance systems, emergency drills.[xvii] At the same time, public officials face a recalibrated risk landscape. Visibility, once a prerequisite for democratic engagement, now carries heightened personal exposure.[xviii] The cumulative effect is a subtle contraction of civic space, not necessarily in physical terms, but in psychological ones. Trust and safety, once assumed, has now become conditional.

Fragmented Realities

Overlaying these domestic dynamics is a broader global transformation of the fragmentation of shared reality. The contemporary information environment is characterized by abundance, an overproduction of narratives, many of them conflicting. Disinformation, whether state-sponsored or organic, exploits this abundance, eroding confidence in institutions and blurring the boundary between fact and interpretation.[xix] Digital and social media platforms accelerate this process, enabling narratives to move rapidly across borders and communities. Individuals increasingly inhabit distinct informational ecosystems, each reinforcing its own internal logic.[xx] In such conditions, consensus becomes difficult to achieve. Disagreement, once mediated through shared facts, becomes more fundamental, slight perceived differences have become “a threat to democracy” itself. As a result, for some, violence emerges not as a breakdown of communication, but as an alternative to it.[xxi]

Interconnected Risk

One of the defining features of the current environment is not any single factor, but their interaction. Digital and viral social media amplification, institutional distrust, ideological fragmentation, and decentralized mobilization do not operate independently. They reinforce and circularly “inspire” one another.[xxii] This creates a compounding effect. Each incident of violence feeds perception; each perception shapes behavior; each behavior increases the likelihood of further incidents.[xxiii] The result is a feedback loop in which instability becomes self-reinforcing, not just constant, but persistent.

And yet, to focus solely on risk is to miss the ever-constant parallel reality: resilience. Communities continue to function. Institutions continue to operate. In the aftermath of violence, there are acts not only of mourning, but of rebuilding, quiet, often unremarked, but consequential.[xxiv] Schools reopen. Congregations gather. Public life resumes, not unchanged, but intact. There remains a durable

commitment to democratic processes, to nonviolent engagement, and to the idea, however strained, that conflict can be resolved without force.[xxv] Resilience, in this sense, is the capacity to absorb and deflect it.

Conclusion: Managing Risk, Rebuilding Trust

The United States is not descending into chaos, but it is navigating a transformation. Violence has not become ubiquitous, but it has become more *integrated*, more visible, more discussed, and in some cases, more normalized. Addressing this shift requires more than tactical responses. Security measures can mitigate immediate threats, but they cannot alone restore trust or coherence. That work lies elsewhere: in strengthening institutions, improving the integrity of information ecosystems, and addressing the underlying conditions that give violence its resonance. In addition, the persistence of resilience offers a counterweight. The systems that sustain civic life, imperfect but enduring, remain intact. The challenge, then, is not only to manage violence as a risk, but to prevent it from becoming a defining feature of the national identity.

Author: Matt Nieminski is the Director of Intelligence at RMS International and has worked as an intelligence analyst for 15 years at multiple security and technology companies.

Endnotes

[i] Institute for Economics & Peace, "Evolving Threat of Lone Wolf Terrorism in the West," *Vision of Humanity*, March 4, 2025, https://www.visionofhumanity.org/evolving-threat-of-lone-wolf-terrorism-in-the-west/. See also Institute for Economics & Peace findings that lone actors accounted for approximately 93 percent of fatal terrorist attacks in Western countries in recent years.

[ii] For recent examples illustrating the escalation and diversification of political violence in the United States, see coverage of the two assassination attempts against Donald Trump during the 2024 presidential campaign, including the July 13, 2024 shooting at a rally in Butler, Pennsylvania, and a subsequent thwarted attempt in West Palm Beach, Florida; see also the June 14, 2025 targeted shootings in Minnesota resulting in the assassination of State Representative Melissa Hortman and her husband and the attempted assassination of State Senator John Hoffman and his spouse; and the February 2026 suspension of a Minnesota gubernatorial campaign following the fatal stabbing of the candidate's daughter. These incidents, taken together, reflect an increasingly personalized and diffuse threat environment affecting national figures, state-level officials, and political families alike. See "Political Violence in the 2024 United States Presidential Election," "Trial Begins for Man Accused of Trying to Assassinate Trump," *Reuters*, September 11, 2025; "The Attacks on Democratic Lawmakers in Minnesota: What We Know," *The Guardian*, June 14, 2025; and "Minnesota Governor Candidate Ends Campaign After Daughter, 22, Is Found Stabbed to Death," *People.*

[iii] *New York Post*, "Attacks on U.S. Churches Have Risen Significantly Since 2021, Report Finds," September 1, 2025, https://nypost.com/2025/09/01/us-news/attacks-on-us-churches-have-risen-significantly-since-2021-report-finds/. See also Family Research Council, "Hostility Against Churches in the United States: 2018–2024," which identifies 1,384 incidents targeting churches between January 2018 and December 2024, with a marked escalation beginning in 2022 and sustained elevated levels through 2023–2024.

[iv] Recent attacks on houses of worship in the United States illustrate the continued targeting of religious institutions across differing faith communities. On January 28, 2026, a vehicle-ramming incident at the Chabad–Lubavitch World Headquarters in Brooklyn, New York, was investigated as a potential

antisemitic hate crime after a driver repeatedly struck the synagogue's entrance, prompting heightened security measures citywide; see "Chabad Headquarters Car Ramming Attack," January 28, 2026. In a separate incident, a mass shooting and arson attack at a meetinghouse of the Church of Jesus Christ of Latter-day Saints in Grand Blanc Township, Michigan, on September 28, 2025, resulted in multiple fatalities and injuries and was linked to anti-religious animus toward the LDS community; see "2025 Grand Blanc Township Church Attack." More broadly, federal authorities have identified continued threats to Jewish institutions, including a March 12, 2026 vehicle-ramming and shooting attack at Temple Israel in Michigan, later characterized by the FBI as a Hezbollah-inspired act of terrorism. Together, these incidents underscore a pattern of ideologically diverse but converging threats against religious targets in the United States, reinforcing concerns regarding the vulnerability of houses of worship in an increasingly volatile domestic threat environment.

[v] Arendt, Hannah. *On Violence*. New York: Harcourt, Brace & World, 1970.

[vi] Bandura, Albert. "Social Cognitive Theory of Mass Communication." *Media Psychology* 3, no. 3 (2001): 265–299.

[vii] Bauman, Zygmunt. *Liquid Modernity*. Cambridge: Polity Press, 2000.

[viii] On the increasing normalization and, in some cases, online endorsement or glorification of political violence in Western democracies, see Anti-Defamation League, "Hate, Extremism, and Terrorism in the United States," 2024; U.S. Department of Homeland Security, *Homeland Threat Assessment 2024* (Washington, DC: DHS, 2024); and Institute for Strategic Dialogue, "The Online Ecosystem of Extremism," 2023. These reports document a growing trend in which acts of violence are framed within supportive or justificatory narratives in digital spaces, including the celebration of attackers, such as Tyler Robinson and Luigi Mangione, the rapid dissemination of manifestos or symbolic content, and the emergence of decentralized communities that legitimize or encourage violence against political or ideological opponents.

[ix] Recent true crime documentaries and dramatizations centered on perpetrators have attracted mass global audiences, reinforcing their cultural prominence and extending public engagement with violent actors. Netflix's *The Menendez Brothers* drew approximately 22.7 million views in its first week and ranked as the platform's most-watched film globally, while *Monster: The Lyle and Erik Menendez Story* generated over 12 million weekly views and trended in dozens of countries, accompanied by renewed public sympathy campaigns. Similarly, *Monster: The Ed Gein Story* reached more than 12 million views within three days and surpassed 20 million views in its second week, maintaining a multi-week presence in global rankings. The earlier *Monster: The Jeffrey Dahmer Story* achieved even greater scale, becoming one of Netflix's most-watched series and accumulating hundreds of millions of viewing hours worldwide. Although exact figures are less publicly disclosed, *Killer Inside: The Mind of Aaron Hernandez* has remained a consistently promoted and widely consumed title, indicating sustained long-tail engagement. Collectively, these viewership patterns demonstrate that perpetrator-focused narratives now reach tens of millions of viewers per release cycle, sustaining prolonged visibility and, in some cases, contributing to the reinterpretation or humanization of violent offenders within popular media ecosystems.

[x] An American Psychological Association review found that media coverage of violence can increase the likelihood of similar acts shortly after exposure. https://www.apa.org/topics/video-games/violence-harmful-effects

[xi] Berger, J. M. *Extremism*. Cambridge, MA: MIT Press, 2018.

[xii] On the emergence of online sympathy and justificatory narratives surrounding perpetrators of political violence, including reactions to the 2025 assassination of Charlie Kirk and comparable cases, see reporting and analysis noting that public discourse across digital platforms has included expressions of support, ironic endorsement, and ideological framing of suspects such as Tyler Robinson, as well as parallel online support dynamics in cases involving Luigi Mangione. See Richard Luscombe, "Prosecutors

Seek Death Penalty for Suspect in Charlie Kirk Assassination," *Reuters*, September 16, 2025, and subsequent coverage of the case's widespread online attention and politicized reactions; see also "Why More Young Americans Are Cheering for Violence," *The Times*, October 31, 2025, which documents attitudinal shifts among subsets of younger Americans expressing approval or ambivalence toward politically motivated violence; and Network Contagion Research Institute (NCRI), analysis of survey and behavioral data indicating that support for acts such as the assassination of public figures correlates with broader acceptance of political violence and is reinforced within digital ecosystems. These findings suggest that sympathy for perpetrators—whether explicit or coded—has become part of a wider pattern of normalization and ideological justification of violence in fragmented online environments. Benkler, Yochai, Robert Faris, and Hal Roberts. *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics*. New York: Oxford University Press, 2018.

[xiii] Durkheim, Émile. *The Division of Labor in Society*. New York: Free Press, 1997.

[xiv] Fisher, Max. *The Chaos Machine: The Inside Story of How Social Media Rewired Our Minds and Our World*. New York: Little, Brown, 2022.

[xv] Foucault, Michel. *Discipline and Punish: The Birth of the Prison*. New York: Vintage Books, 1977.

[xvi] Girard, René. *Violence and the Sacred*. Baltimore: Johns Hopkins University Press, 1977.

[xvii] Jenkins, Brian Michael. *Will Terrorists Go Nuclear?* Amherst, NY: Prometheus Books, 2008.

[xviii] Klinenberg, Eric. *Heat Wave: A Social Autopsy of Disaster in Chicago*. Chicago: University of Chicago Press, 2002.

[xix] Merton, Robert K. *Social Theory and Social Structure*. New York: Free Press, 1968.

[xx] Mudde, Cas, and Cristóbal Rovira Kaltwasser. *Populism: A Very Short Introduction*. Oxford: Oxford University Press, 2017.

[xxi] Putnam, Robert D. *Bowling Alone: The Collapse and Revival of American Community*. New York: Simon & Schuster, 2000.

[xxii] American Psychological Association, "Violence in the Media: Psychologists Study Potential Harmful Effects," accessed April 1, 2026, https://www.apa.org/topics/video-games/violence-harmful-effects. See also Craig A. Anderson et al., "The Influence of Media Violence on Youth," *Psychological Science in the Public Interest* 4, no. 3 (2003): 81–110, which finds that exposure to violent media increases the likelihood of aggressive thoughts and behaviors in both immediate and short-term contexts; and L. Rowell Huesmann, "The Impact of Electronic Media Violence: Scientific Theory and Research," *Journal of Adolescent Health* 41, no. 6 (2007): S6–S13, documenting that even brief exposure to violent content can elevate the risk of aggressive behavior shortly after viewing. Collectively, this body of research supports the conclusion that media coverage and depictions of violence can contribute to short-term increases in aggressive or imitative behaviors following exposure. Sunstein, Cass R. *#Republic: Divided Democracy in the Age of Social Media*. Princeton, NJ: Princeton University Press, 2017.

[xxiii] Tufekci, Zeynep. *Twitter and Tear Gas: The Power and Fragility of Networked Protest*. New Haven, CT: Yale University Press, 2017.

[xxiv] U.S. Department of Homeland Security. *Homeland Threat Assessment 2024*. Washington, DC: DHS, 2024.

[xxv] Weber, Max. *Economy and Society*. Berkeley: University of California Press, 1978.

Book Review

Book Review: The Protector's Edge: Leadership Through Strategy and Action By Chuck Randolph, Jonathan Wackrow, and Fred Burton

Reviewed by Jeff M Moore, PhD

The Protector's Edge: Leadership Through Strategy and Action is not another executive protection book about motorcades, advance work, formations, routes, residences, protective details, or the mechanics of moving a principal from point A to point B. Of course, these things still matter, and always will, but Chuck Randolph, Jonathan Wackrow, and Fred Burton are focused on something larger, more urgent, and more sophisticated: the transformation of the protection professional into a strategic, intelligence-led leader who helps protect not only people, but organizations, brands, reputations, decision-making systems, and corporate resilience.

The authors argue that the modern protection model has changed fundamentally. The old model—guns, guards, gates, and proximity—is no longer enough. A protector can still be physically close to a principal and strategically irrelevant to the organization. That is a hard truth, but it is one of the central lessons of this book. Today's threats are multifaceted. They include physical, cyber, reputational, and informational domains. A hostile actor may not begin with a weapon. He may begin with a grievance, an online narrative, a doxxing campaign, a deepfake, a protest call, a reputational attack, a leak, a cyber intrusion, or an ideological mobilization effort. The physical attack, if it comes, may be the end of a chain rather than the beginning. That is where The Protector's Edge becomes especially important.

The book repeatedly pushes the reader away from reactive protection and toward anticipatory leadership. The authors are not dismissing tactical competence. They are saying tactical competence is the baseline. It is the admission ticket. It is not enough to earn sustained influence in the C-suite, with boards, or across legal, communications, human resources, cyber, operations, and business units. The modern protector must understand the principal AND their corporation. He or she must understand how the organization makes money, how it communicates, how it is perceived, where it is vulnerable, how its leaders think, what keeps the CEO awake at night, and how cyber, political, and security incidents can become operational, reputational, legal, and financial crises. This is a significant shift from traditional executive protection.

In applied terms, the protection leader is no longer simply guarding the executive. The protection leader is helping safeguard the mission, which includes the executive, yes, but also what the executive commands. That means they are protecting the company, plus its product or services, revenues, employees, and brand or reputation. That requires intelligence, judgment, diplomacy, emotional control, business fluency, initiative, and the ability to influence without formal authority.

One of the book's strongest contributions is its treatment of the "protector-leader." It captures the professional evolution the authors are describing. The protector-leader is not a knuckle-dragging stereotype with an earpiece and a gun. Nor is he solely a former operator who has been promoted into a management slot. The protector-leader is closer to a hybrid intelligence officer, risk advisor, crisis manager, business enabler, and protective strategist all rolled into one. At times, the model described in the book resembles a combination of a domestic and international intelligence service embedded inside a corporation, like a joint MI5/MI6 type unit. That is not an exaggeration. The modern corporate protection function must understand threats, intentions, capabilities, tactics, ideology, grievances, online mobilization, physical attack Tactics, Techniques and Procedures (TTPs), reputational vulnerabilities and organizational consequences. Ideally, it must convert that understanding into action before the crisis erupts. And, inevitably, when crisis does erupt, it must act nimbly and decisively to mitigate the threat. That is intelligence work.

The authors make this point through multiple case studies and leadership frameworks. Their discussion of the Elon Musk doxxing incident is particularly effective. The incident was not just a privacy issue or a physical security problem. It was a hybrid threat attack involving personal exposure, online hostility, family safety, investor confidence, public perception, law enforcement liaison, legal takedown efforts, cyber investigation, public relations, and physical protection. The protective response had to be fast, cross-functional and intelligence-led. That is the new operating environment.

The book's treatment of the Brian Thompson assassination is also important because it links grievance, ideology, online narrative, and targeted violence. This is a critical insight for the protection profession. Assassination culture does not emerge in a vacuum. It can be fed by grievance, amplified by online communities, rationalized by ideology, and normalized by digital narratives before it becomes physical violence. Protectors must therefore learn to monitor not only the attacker's weapons and access points, but also the attacker's worldview, grievance structure, digital behavior, propaganda environment, and escalation pathway. That means protective intelligence must extend well beyond traditional threat lists and known bad actors. It must examine the strategic threat picture in which violence becomes thinkable, attractive, or socially popular. For security professionals, that is one of the most important lessons of the book.

The authors also make a strong case that protection must be integrated into corporate decision-making. Security leaders who remain outside the business ecosystem will always struggle for relevance. Staying on the outside reinforces the common corporate view that security is a cost center and is therefore less relevant. Security leaders who understand the business, on the other hand, can frame risk in terms the organization already understands: revenue, continuity, reputation, litigation, regulation, investor confidence, employee safety, and brand resilience. This is a key takeaway from the book, and the authors explain it most convincingly.

A tactical operator may say, "We need more coverage because the threat environment is escalating." A protector-leader says, "Our current threat exposure increases operational and reputational risk. We can reduce that risk through targeted protective measures aligned with business continuity priorities." That difference is neither semantic nor esoteric. It is the difference between being seen as a cost center and being treated as a strategic advisor. Chapter 2, "From Executive Protection to Executive Presence," is especially useful in this regard. The chapter explains the difficult transition from tactical excellence to strategic influence. Many protectors are highly competent in the field but less comfortable in the boardroom. And, importantly, the authors do not simply explain that gap. They prescribe how to close it, which makes the book even more groundbreaking.

Their advice is direct and practical: learn the business as your new area of operation. Build business fluency into your briefings. Create early wins with legal, HR, operations, communications and other internal partners. Track your leadership development with the same discipline used to track a protection detail. Study resistance. Record lessons. Reflect. Adapt. That is excellent guidance. In this regard, the book's discussion of TJ Klump's evolution at Amazon is one of the stronger case studies because it shows how a protection professional can move from tactical expertise into enterprise security leadership. The key lesson is that Klump and leaders like him made themselves relevant to the business, not just the threat. That sentence could almost serve as one of the book's central operating principles. The protector who understands only the threat will remain a specialist. The protector who understands the threat, the principal, AND the business can become indispensable to the corporate mission.

The leadership chapters are also valuable because they broaden the discussion beyond protective intelligence. The authors emphasize character, humility, trust, emotional composure, operational vigilance, dynamic decision-making and strategic credibility. These are not soft concepts. In a crisis, they become operational requirements. For example, the book asserts:

- A leader who lacks emotional control can infect the team with panic.
- A leader who lacks humility will miss weak signals and dissenting views.
- A leader who lacks credibility will not be trusted when rapid decisions are required.
- A leader who lacks strategic clarity may win the immediate tactical moment and still lose the broader organizational fight.

This is where the book does a good job connecting leadership theory to protective practice. Mission command, adaptive leadership, servant leadership, influence without authority, cross-functional trust and team development are not presented as abstract academic ideas. They are treated as practical tools for building protection programs that can survive real stress.

Beyond direct leadership principles, the book also explains how to take on the correct mindset. For example, Chapter 4, "Leadership Mindset: From Reactive to Proactive," may be one of the most important chapters for working protection professionals. The core argument is that proactive leadership is about seeing risk before it surfaces and shaping the environment before the threat controls the tempo. The best protection work is often invisible. The successful advance, the adjusted route, the delayed press release, the alternate venue, the quiet law enforcement coordination, the early detection of hostile sentiment, the decision to reduce exposure before a crowd forms. These actions rarely generate dramatic stories, but they prevent emergencies, reputational damage, injuries and deaths.

The book's case study involving a Brazilian energy executive traveling to West Africa is a strong example of predictive, intelligence-led protection, *and intelligence is a constant theme throughout the book*. The security leader in this case did not wait for the trip to become dangerous. She began months in advance, conducting a dynamic threat and vulnerability assessment that included geopolitical analysis, maritime security, social sentiment, activist mobilization, and local militia risk. She then used that intelligence to adjust the venue, shape communications, and reduce her principal's exposure before the adversary could exploit the original protection plan. That lesson is the essence of strategic risk management.

The same logic applies to the book's broader discussion of converged threats. Physical security, cyber security, legal response, communications strategy, employee sentiment, social media narratives, and

executive decision-making now intersect. A reputational attack can create a physical threat. A cyber leak can create a protest. A protest can create an assassination opportunity. A deepfake can create financial loss, public outrage, or personal danger. These are not separate problems anymore. They are connected threat systems, and the protection profession must build connected response systems.

That is why the book's discussion of the protector-leader as an orchestrator of the organization's "risk immune system" is so useful. The best security leaders do not simply react when the alarm sounds. They help build the organizational tissue that detects, interprets, communicates and responds before damage spreads. They connect cyber, legal, HR, communications, operations and physical security before the adversary forces that integration during a crisis. That is mature protection.

The book is also strong on resilience. It recognizes that protection is not only about stopping bad things from happening. It is about helping organizations absorb shock, maintain continuity and recover quickly when threats materialize. That is a crucial point for corporate security, government security, family office protection, event security and protective intelligence teams. Resilience is part of the protective mission.

If there is a broader professional lesson in The Protector's Edge, it is that the protection field is at an inflection point. The profession can remain attached to older images of executive protection—the visible guard, the tactical specialist, the driver, the close-in protector—or it can expand into a more sophisticated intelligence-led discipline that supports enterprise risk, leadership continuity and organizational trust. The authors clearly favor the second path. They are right to do so.

Security professionals should read this book because it explains where the profession is going. More importantly, it explains what kind of person the future protection leader must become. That person must still respect the fundamentals. He must know the route, the room, the crowd, the exits, and the attack surface. But he must also know the principal's business, the organization's culture, the online narrative environment, the legal and reputational implications of security decisions, and the strategic consequences of getting it wrong. That is a much higher standard. It is also the correct standard, one that will lead the way in an increasingly complex threat environment.

The Protector's Edge is ultimately a book about professional maturation. It is about moving from reaction to anticipation, from proximity to influence, from tactical execution to strategic judgment, and from guarding people to enabling resilience. For protectors, security leaders, intelligence professionals, risk managers and executives, the book is not merely useful. It is timely and groundbreaking. The modern threat environment is faster, more ideological, more networked, more public and more unforgiving than the old one. The protection profession must evolve accordingly. This game changing book shows how.

Author: Dr. Jeff Moore is the CEO of Muir Analytics, which conducts threat assessments for corporations. Dr. Moore created the company's flagship product, the SecureHotel Threat Portal, which is the largest hotel violence database. Dr. Moore earned his PhD in counterinsurgency/counterterrorism from the University of Exeter in the UK, and he is the author of *Spies for Nimitz* and *The Thai Way of Counterinsurgency*.

Interview with Experts

Protective Intelligence, Professionalization, and the Future of Security: An Interview with Jenni Randolph

Jenni Randolph is a highly regarded leader in corporate security and protective intelligence whose career has been defined by building and operationalizing intelligence-driven security programs at scale. Currently serving as Director of Global Security Risk at Roku, Jenni has had prior security leadership positions at companies such as Twitter and Amazon. She has consistently worked at the intersection of executive protection, global events security, and intelligence analysis, providing both strategic direction and operational support to high-risk environments. Earlier in her career, she spent over a decade at Concentric Advisors, where she built a protective intelligence capability from the ground up, developing threat assessment processes, and managing large-scale investigative programs, including a robust persons-of-interest database. Beyond her corporate roles, Randolph has been deeply involved in advancing the field through organizations such as the Association of Threat Assessment Professionals and the International Protective Security Board, mentoring practitioners and contributing to the evolution of professional standards. She is being featured in this interview not only for her technical expertise, but for her quiet, sustained, and highly impactful contributions to the security profession, particularly her role in shaping practitioner communities and elevating industry dialogue through forums such as the Close Protection Conference, where her influence is felt as much in structure and substance as it is in outcomes.

Protective Intelligence

Interviewer: Your career has primarily focused on protective intelligence and executive protection. Over the past decade, how has protective intelligence shifted in terms of methodology, not just tools? Importantly, what are teams still getting fundamentally wrong?

Jenni: One of the biggest changes I've seen is the growth of dedicated protective intelligence teams. Early in my career, many organizations outsourced that function or treated it as something separate from executive protection. Today, more companies have internal protective intelligence capabilities, and those teams are increasingly embedded with executive protection operations. That's a huge improvement.

Historically, intelligence teams and executive protection teams often operated in separate lanes. They didn't always communicate effectively, and intelligence products weren't always aligned with what the protection team actually needed. Today, analysts are traveling with protection teams, participating in advances, and contributing directly to operational planning. That's where protective intelligence has the greatest value.

The mistake many organizations still make is treating protective intelligence as simply threat investigation. That's only part of the job. Analysts need to understand the principal, where they're going, what matters to them, and what information the protection team needs to make decisions. Intelligence only matters if it can be operationalized.

The next frontier is digital executive protection. An executive's digital footprint increasingly creates physical risk, yet many organizations still don't fully understand that relationship. Some teams are beginning to adopt digital EP tools and methodologies, but many are still missing that piece. Analysts are uniquely positioned to bridge that gap, and I think we'll see that become a much larger part of executive protection programs in the coming years.

Interviewer: Many organizations claim to have “protective intelligence” capabilities. In your view, what distinguishes a true protective intelligence program from basic monitoring or threat awareness?

Jenni: A true protective intelligence program looks at the entire threat ecosystem surrounding an organization and its people. It's not just monitoring social media or watching locations where executives happen to be.

The first question is whether you're actually capturing all the threat streams. Are you reviewing physical mail, voicemails, threats made at events, and information coming through customer service channels? Threats emerge through many different vectors, and mature programs have mechanisms to collect and evaluate all of them.

The second distinction is integration. Protective intelligence cannot operate in isolation. It needs to be closely connected to executive protection, physical security, legal, human resources, and operational teams. The more integrated the program is, the more effective it becomes.

Finally, true protective intelligence is proactive rather than reactive. It's not just identifying threats after they appear. It's helping reduce risk before a threat materializes. That includes privacy protection, vendor vetting, digital exposure management, and understanding how an executive's activities create vulnerabilities. The best programs focus on prevention as much as detection.

Interviewer: How should protective intelligence integrate with physical security and executive protection operations in a way that actually changes outcomes, not just reporting?

Jenni: One of the most effective things an organization can do is put analysts in the field alongside executive protection teams. When a large detail is traveling or supporting a major event, having an analyst on the ground can be a game changer.

An analyst sitting in an office can certainly gather information and produce intelligence products. But when they're physically present—talking to local law enforcement, observing the environment, understanding routes, and seeing issues firsthand—they gain a much deeper understanding of the operational picture.

That experience also improves the analyst's ability to support future operations. An analyst who has never worked alongside protection agents may not fully understand which data points actually matter in the field. Spending time with operators helps close that gap.

When I was at Concentric, I had opportunities to travel extensively and support operations around the world. Sometimes that meant assessing threats, and sometimes it meant understanding seemingly small details, such as where agents could safely operate or where local patterns might affect movement. Those experiences made me a better intelligence professional because they connected the analysis directly to operational reality.

Professionalization of Security

Interviewer: Organizations like the Association of Threat Assessment Professionals (ATAP), ASIS International, and the International Protective Security Board play a growing role in shaping the field. Where have they been most effective in advancing professional standards?

Jenni: These organizations were founded by practitioners asking a simple question: How do we make this profession better? One of their greatest contributions has been providing access to training, research, and professional development. They regularly bring together experienced practitioners, academics, and researchers to share insights and best practices. In many cases, they make those resources broadly accessible to the profession.

Over the last twenty years, they've also become invaluable networking hubs. Security professionals often work in highly specialized environments and can become isolated within their own organizations. These associations create opportunities to connect with peers, exchange ideas, and learn how others are solving similar problems.

Perhaps most importantly, they've helped create and refine professional standards. There are now communities actively working to identify best practices and establish frameworks that security professionals can apply within their organizations. Without these groups, many of us would have far fewer opportunities to stay current on emerging trends and evolving methodologies.

Interviewer: Where do these organizations fall short, particularly in bridging the gap between theory, standards, credentials, and operational competence?

Jenni: Protective intelligence is somewhat unique because many of its methodologies have been developed, tested, and refined over decades. There are strong frameworks for threat assessment, behavioral analysis, and risk management, and some certifications reflect that depth of rigor. For example, ATAP's Threat Management credential is exceptionally demanding. It's difficult to earn, but that difficulty gives it meaning.

The challenge is that not all credentials are equal. Some certifications have decades of validation behind them, while others do not. The industry does a bit of a disservice by not doing a better job of helping people distinguish between credentials that reflect deep expertise and those that are primarily educational experiences.

There's also a broader challenge. While many aspects of protective intelligence and executive protection can be standardized, there will always be significant variation between organizations. Every company has a different culture, risk profile, leadership team, and operating environment.

I've held multiple security roles throughout my career, and while the foundational principles remained the same, the way I applied them differed dramatically. A certification or training program can teach fundamentals, but it cannot tell you exactly how to operate within every corporate environment. In that sense, security will always require a degree of creativity, judgment, and adaptation.

Interviewer: Do you believe the security field is meaningfully closer to being a true profession, or does it still operate more like a trade?

Jenni: I absolutely think we've become more professionalized over the last twenty years. When I first entered the field, there was often a disconnect between corporate security professionals and law enforcement. Today, many law enforcement agencies have personnel trained in threat assessment and behavioral analysis, creating a much stronger foundation for collaboration.

We're also seeing organizations take a far broader view of risk. Twenty years ago, executive protection often meant assigning someone to stand next to an executive. Today, mature programs incorporate protective intelligence, threat assessment, digital risk monitoring, crisis management, and a much more comprehensive understanding of the threat landscape.

We're no longer just throwing bodies at problems. We're applying analysis, intelligence methodologies, and structured risk management. That doesn't mean we've fully matured as a profession, but we've unquestionably moved in that direction.

Career Development and Tradecraft

Interviewer: For someone who has built a career entirely within private security, what advantages and blind spots does that pathway create compared to government or military backgrounds?

Jenni: One advantage is that I came into the profession without many preconceived notions about how security "had" to be done. I wasn't trained in a government agency that prescribed a specific way of approaching every problem. Instead, I learned within the realities of the private sector, where solutions often need to be adapted to the culture, priorities, and risk tolerance of the organization.

That experience has made me more flexible. Corporate security is nuanced. What works for one company, executive, or industry may not work for another. Because I grew up professionally in that environment, I've always approached problems by asking what works best for the business rather than relying on a particular institutional model.

People are often surprised that I don't have a government or military background. There is a perception in parts of the industry that those backgrounds are required, but I don't think that's true. In fact, private-sector professionals often develop a strong understanding of how businesses operate and how security functions need to align with broader organizational objectives.

The challenge, however, is that much of the security industry is still populated by people who came from government or military careers. They often share similar training, experiences, and professional assumptions. As someone without that background, I was sometimes an outsider.

There were certainly areas where I had to work harder. I wasn't trained as an intelligence analyst through a government program. I didn't come into the profession with the same operational experiences that many of my peers had. At the same time, those differences created opportunities for mutual learning. I've learned from colleagues with government backgrounds, and I've often helped them understand how the private sector operates differently.

One of the biggest transitions many former government professionals face is realizing that corporate security is fundamentally different from government security. The mission, stakeholders, constraints, and success metrics are different. Learning how to navigate that environment is just as important as any operational skill.

Interviewer: What specific skills, disciplines, or areas of study have had the highest return on investment in your career?

Jenni: My master's degree was incredibly valuable. As an undergraduate, I was often told it wouldn't matter, but it became an important credential and helped open doors throughout my career.

Beyond formal education, studying threat assessment had a tremendous impact. Early in my career, I wasn't familiar with the body of research surrounding threat assessment and behavioral analysis. Through organizations like ATAP, I immersed myself in the literature, methodologies, and research that practitioners had developed over decades.

That changed the way I approached risk. Instead of relying on intuition, I had frameworks for evaluating behavior, identifying warning signs, and assessing threats in a structured way. It gave me confidence that my recommendations were grounded in established research rather than personal judgment.

Executive protection training was also valuable. While my career has primarily focused on intelligence and threat assessment, taking executive protection courses helped me better understand the operational side of the business. It made me a stronger analyst because I understood what operators actually needed and how intelligence was being applied in the field.

That said, the most important skills I've developed are probably soft skills. Collaboration has had the highest return on investment of anything I've learned. Security is ultimately a team sport. You have to work effectively with executive assistants, legal teams, HR, communications professionals, IT teams, and business leaders.

Responsiveness is another underrated skill. When people feel heard and supported, they're more likely to work with you and trust your judgment. It sounds simple, but building strong professional relationships has probably been as important to my career as any technical competency.

Interviewer: If you were designing a modern curriculum for security professionals, what would be non-negotiable components?

A modern security curriculum needs to expose students to the full spectrum of corporate security disciplines. That includes security operations, access control, executive protection, protective intelligence, geopolitical intelligence, crisis management, event security, and physical security fundamentals. But I think many people underestimate the importance of business knowledge.

Future security leaders need to understand budgeting, strategic planning, forecasting, program management, and business operations. They need to understand how organizations function and how decisions are made. Security professionals don't operate in a vacuum; they operate within businesses. I would also want students to learn how to work effectively with functions such as legal, communications, human resources, and information technology. The ability to collaborate across departments is incredibly important.

Another area that deserves more emphasis is risk management. Security professionals need to understand that different stakeholders view risk differently. What security sees as a security issue may be viewed as a

reputational issue by communications, a legal issue by attorneys, or an operational issue by business leaders.

Understanding those perspectives allows security professionals to communicate more effectively and build solutions that work for the entire organization rather than just the security department.

Leadership and Organizational Design

Interviewer: What leadership principles are most critical for security professionals who are transitioning from operator roles into leadership positions?

Jenni: One of the biggest shifts is learning to think beyond operations and understanding the business side of security. Being a great operator doesn't automatically make someone a great leader. As a leader, you're no longer focused solely on executing tasks. You're responsible for strategy, team development, resource allocation, stakeholder management, and long-term program growth.

Collaboration is probably the most important leadership principle. Security leaders must build relationships across the organization and learn how to influence people who don't report to them. Success often depends on your ability to work effectively with other business units.

Decision-making is another critical skill. As you move into leadership roles, you encounter fewer situations that have obvious right or wrong answers. Many decisions involve competing priorities, incomplete information, and uncertain outcomes. You have to be comfortable making difficult decisions while considering their impact on the organization, the business, and your team.

People management is equally important. Many security professionals spend years developing technical expertise but receive very little training on managing people. Hiring, developing talent, writing job descriptions, making headcount requests, and coaching employees are all critical leadership responsibilities that require a different skill set than operational security work.

Interviewer: How should organizations be identifying and developing future leaders in security today?

Jenni: The qualities aren't all that different from what you'd look for in any profession. I look for people with passion, drive, creativity, and strong interpersonal skills. I pay attention to how they solve problems, how they work with others, and whether they can influence outcomes without relying on authority. Security teams need to be viewed as trusted partners within their organizations. Future leaders are often the people who can build those relationships and help others reach solutions rather than simply enforcing policies.

When it comes to development, leadership modeling is incredibly important. Young professionals need opportunities to observe good leadership in practice. But they also need opportunities to grow themselves.

That means giving people stretch assignments and exposing them to challenges that force them to think differently. If you're overly prescriptive and tell people exactly what to do every step of the way, they never develop their own judgment.

One thing I try to do is explain the "why" behind decisions. Instead of simply assigning a task, I want people to understand the broader objective. What are we trying to accomplish? Why does it matter? What larger

problem are we trying to solve? That context helps people develop strategic thinking skills and prepares them for future leadership roles.

However, not everyone wants to be a manager, and that's okay. Organizations need career pathways for highly skilled analysts, investigators, and specialists who want to remain technical experts. Managing people and being an exceptional practitioner are different skill sets. Too often organizations assume that advancement means moving into management. We need to create opportunities for professionals who want to continue growing without necessarily becoming people leaders.

Strategic Outlook

Interviewer: Looking ahead five to ten years, what structural changes do you expect in the security profession, and what should practitioners be preparing for now?

Jenni: I think the profession will continue becoming more sophisticated and more integrated into business decision-making. Over the last twenty years, security has evolved from a largely reactive function into a strategic risk-management discipline. That trend will continue. Organizations expect security leaders to understand business operations, contribute to organizational resilience, and help navigate complex risk environments.

The challenge for practitioners is ensuring that security is viewed as a strategic partner rather than simply a cost center. To get there, we need to become more business-savvy. We need to understand how organizations create value, how executives make decisions, and how security supports broader business objectives. The more effectively we can connect security outcomes to organizational success, the more influence and credibility the profession will gain.

Ultimately, I think the future belongs to security professionals who can bridge the gap between operational expertise and business leadership. Those individuals will be best positioned to shape the next generation of corporate security programs.

Tools for Security Professionals

Tools for Security Professionals is a practical, application-focused section of *The Close Protection and Security Journal* dedicated to how tools are actually used in the field, not how they are marketed or theoretically described. This section examines emerging technologies, established platforms, and legacy tools through an operational lens, emphasizing how security professionals can integrate them effectively into close protection, intelligence analysis, and risk management under real-world constraints. Rather than showcasing novelty for its own sake, the focus is on utility, limitations, and the conditions under which a tool meaningfully improves decision-making, detection, response, or resilience. Contributions to Tools for Security Professionals are written by experienced practitioners and subject-matter experts who understand that tools do not replace judgment, tradecraft, or leadership. Each piece explores how a specific tool or capability can be adapted, combined, or repurposed to solve practical problems, whether that involves leveraging new emergency communications technology, applying analytical software to protective intelligence, or using long-standing methods in unconventional ways.

Investigative Analytics in Practice: Lessons from the Field Using Alteryx, Tableau, & i2

Tromila Maile

My career as a financial investigator began in 2010, and as one might imagine, the tooling for completing such investigations has changed ineffably in the ensuing decades. The reality of modern investigations is that the challenge is rarely a lack of information. More often, the challenge is the opposite. Investigators today are inundated with data from financial records, communication platforms, open-source intelligence, travel records, access logs, customer databases, social media, and a host of other sources. The question for investigators and analysts is how to transform large volumes of disparate information into actionable intelligence. The tools discussed below have each played a role in solving different parts of that problem.

i2 Analyst Notebook

My tried and true tool in my toolbox, which was the first investigation tool I learned to use as well as useful in the last month of my investigations, was i2 Analyst Notebook. While it is easy to describe the persons who have the most activity or the widest range of activity, that does not necessarily mean the investigator has found a central node. The social network analysis completed by i2 is helpful in identifying persons of interest who might not immediately stand out as power users. The visual graphs provided by i2 can be helpful when shifting from the analysis stage of the investigation to the presentation stage when the customer wants the bottom line understanding rather than the details of the process.

One of the greatest strengths of i2 is its ability to reveal relationships that would otherwise remain hidden in spreadsheets and databases. Humans are remarkably good at recognizing patterns visually, but relatively poor at identifying those same patterns when presented as thousands of rows of structured data. Link analysis transforms abstract data into understandable networks. It allows investigators to identify brokers, intermediaries, facilitators, and key connectors whose importance may not be reflected by transaction volume alone.

This distinction is particularly important in financial crime investigations. The individual moving the most money is not always the individual directing the activity. Likewise, the person with the most communications may simply be performing an administrative role. Network analysis helps investigators distinguish between activity and influence. In many cases, the most valuable investigative lead emerges from identifying a seemingly peripheral actor who serves as a bridge between otherwise disconnected groups.

The visual nature of i2 also makes it particularly useful when briefing executives, attorneys, law enforcement partners, or corporate leadership. Investigative professionals often spend weeks or months developing an understanding of a network. Stakeholders, however, typically have minutes. A well-constructed link chart can communicate the essential findings of an investigation far more effectively than a lengthy narrative report.

Tableau

The next tool that has been invaluable throughout my career has been Tableau. I prefer it to Power BI, mostly due to familiarity, not for any quantifiable reason. These tools provide support during both the

analysis and presentation phases of an investigation. For anyone wholly new to these tools, it is apt to think of them like pivot tables on steroids. Whereas Excel operates well up to approximately 50,000 rows, significantly more than that will often cause it to crash if you are doing advanced analysis. Tableau can handle millions of rows in seconds, increasing the efficiency of large-scale investigations. With a single click, the investigator can then convert these pivot tables into a range of graphs. Tableau also has powerful mapping capabilities, which can be particularly useful in the presentation stage. The customer can digest far more information with a well-wrought image than with any number of tables.

For investigators, Tableau's greatest value lies in exploratory analysis. During the early stages of an investigation, the investigator often does not know exactly what they are looking for. Instead, they are attempting to identify anomalies, trends, concentrations, or outliers that warrant further examination. Tableau allows data to be sliced and filtered across multiple dimensions almost instantaneously. Questions that previously required hours of spreadsheet manipulation can often be answered in seconds.

Geographic analysis is particularly valuable in protective intelligence and security investigations. Mapping transaction locations, travel activity, incident reports, or communication patterns can reveal clusters and trends that are difficult to identify through tabular data alone. The ability to visualize activity spatially often produces insights that would otherwise be missed entirely. The presentation capabilities of Tableau are equally important. Investigations frequently culminate in decision-making. Whether the audience is a corporate executive, a security director, an attorney, or a law enforcement partner, the goal is to facilitate understanding. Effective visualizations reduce cognitive burden and allow stakeholders to focus on implications rather than deciphering raw data.

Alteryx

The final tool, that I have used in a smaller number of instances but has been indispensable in those instances, was Alteryx. This is most useful in investigations in which there is a large amount of data that is fat fingered or prone to a variety of structures and/or spellings. An excellent example of when Alteryx saved hours of analysis was during investigations that relied heavily on physical addresses. When writing addresses, people abbreviate roads, acronyms, and cities. They may add or remove commas, and they might switch the place in which the ZIP code appears, especially when addresses from multiple countries are included in the same investigation. Unlike the previous two tools, I used Alteryx exclusively during the analysis stage of the investigation.

One of the enduring truths of investigations is that data quality is often the limiting factor. Before an investigator can identify patterns, relationships, or anomalies, the underlying data must be cleaned and standardized. This is often the least glamorous stage of the investigative process, but it is frequently the most important. Poor data quality can conceal connections, create false negatives, and undermine confidence in analytical findings.

Alteryx excels at automating many of these tasks. Address standardization, duplicate detection, fuzzy matching, and record normalization can be completed at a scale that would be impractical through manual review alone. Investigators often receive data from multiple organizations, systems, and jurisdictions, each of which may use different formatting conventions. Alteryx allows these disparate datasets to be transformed into a common structure suitable for analysis.

In many investigations, the workflow naturally progresses from Alteryx to Tableau and finally to i2. Data is first cleaned and standardized, then explored and visualized, and finally transformed into relationship

networks that allow investigators to identify key actors and understand the structure of the activity under examination. Each tool performs a different function, but together they form a powerful investigative ecosystem.

LLMs

In the last year, the tech world has been inundated with artificial intelligence (AI) tools. While not an early adopter of the new tools, I was also not among those who refused to try them. AI has been particularly helpful in situations that would have previously required engineer support to pull data. While not strictly necessary, a basic understanding of SQL and RegEx allowed for maximization of the above tools. I could write queries for joins, unions, and where searches, but anything more complex required hours of Reddit reconnaissance combined with repeated trial and error sessions. AI allowed me to skip those tedious hours by accepting natural language requests and generating the complex SQL for me. What might have taken me four hours to perfect, down to the final comma that was out of place, was now written for me in a matter of minutes. And for projects requiring engineering support from external teams, it reduced weeks of project management into hours of generation and regeneration by myself.

The most immediate impact of large language models has not been replacing investigators but rather lowering technical barriers. Many investigators understand what question they want to ask but lack the specialized coding skills necessary to extract the answer efficiently. AI serves as a translator between investigative intent and technical execution. SQL queries, regular expressions, Python scripts, data transformation workflows, and other technical tasks can now be generated through natural language interactions. This democratization of analytical capability is significant. Investigators can spend less time wrestling with syntax and more time evaluating evidence, testing hypotheses, and developing investigative leads. The productivity gains are often substantial, particularly for analysts who possess enough technical knowledge to recognize when an AI-generated solution is reasonable but not necessarily enough expertise to build the solution from scratch. My analysis was more comprehensive as I could get answers to my complex questions quickly and then ask additional questions to examine the investigation from multiple angles. It has made proactive investigations simpler and faster, increasing both efficiency and effectiveness.

AI has also proven useful for tasks beyond coding assistance. It can summarize large volumes of text, identify themes across documents, assist with report drafting, suggest alternative analytical approaches, and help investigators think through potential explanations for observed patterns. In this sense, AI increases the speed at which investigators can move through the analytical cycle while allowing more time for judgment and decision-making.

The biggest caveat that comes with using AI in investigations is a caveat that should come with using AI anywhere: the information it generates needs to be verified. For data, that means having a source of truth that can be sampled to compare the results of the pull to ones known to be accurate. If responses from the AI seem extraordinary, they probably are and need to be further validated. The use of AI without follow up steps endangers both the investigations and the profession. AI is a tool; it is not an investigator. Therefore, the human behind the investigation should be the final step in any intelligence product. Shipping a result from an AI without verification is the epitome of irresponsibility.

The risks extend beyond simple factual errors. AI systems can misunderstand context, generate plausible but incorrect explanations, misinterpret relationships, or confidently present assumptions as conclusions. These weaknesses become particularly dangerous when investigators are operating under time pressure or when decision-makers are predisposed to accept the output because it appears authoritative. The core

skills of investigation therefore remain unchanged. Critical thinking, skepticism, corroboration, and validation are just as important today as they were before the emergence of AI. In many respects, they are more important. As analytical tools become increasingly powerful, the consequences of uncritically accepting their outputs become increasingly severe.

The future of investigations will almost certainly involve greater integration of artificial intelligence, automation, and advanced analytics. However, the most successful investigators will not be those who blindly embrace every new technology, nor those who reject innovation outright. They will be the investigators who understand both the capabilities and limitations of their tools and who continue to apply sound investigative tradecraft regardless of how sophisticated the technology becomes. Technology may accelerate the investigative process, but judgment remains a uniquely human responsibility.

Author: Tromila Maile is an expert in financial crimes, money laundering, and anti-fraud investigations. She has done work on these subjects and other types of data analytics for the federal government, state government, financial institutions, and technology companies for almost twenty years.

Practitioners' Bookshelf

The Practitioner's Bookshelf is a dedicated section of *The Close Protection and Security Journal* designed to bridge the gap between theory, history, and real-world security practice. Rather than offering traditional academic book reviews focused on literature placement or scholarly debate, this section evaluates books through the lens that matters most to working professionals: what a practitioner can learn, apply, and internalize to become more effective in the field. Each review treats a book as a tool, case study, or framework, examining how its insights translate into decision-making, risk assessment, protective intelligence, leadership, and operational judgment across close protection, corporate security, and intelligence disciplines.

The guiding premise of The Practitioner's Bookshelf is that professional excellence is cumulative and cultivated over time. A serious security professional should maintain a personal bookshelf not as a display of credentials, but as an evolving archive of hard-won lessons drawn from history, strategy, failure, and adaptation. The books reviewed here may come from security studies, geopolitics, psychology, military history, true crime, or even literature, but each is assessed for its practical relevance to protecting people, organizations, and systems under real constraints. This section encourages readers to think critically, learn continuously, and build intellectual depth as deliberately as they build technical skill, reinforcing the idea that judgment, perspective, and disciplined thinking are as essential to protection as any tactic or tool.

Book Review: The Protective Intelligence Advantage: Mitigating the Rising Threat to Prominent People by Fred Burton and Scott Stewart

The literature of intelligence and security contains many books about theory, history, and institutions. There are shelves devoted to the intelligence cycle, analytic methods, counterterrorism, espionage, national security decision-making, and the evolution of state intelligence services. These works are valuable, but they often leave the practitioner with a familiar problem. They explain why intelligence matters without always showing how intelligence is used in the daily work of protecting people. Fred Burton and Scott Stewart's *The Protective Intelligence Advantage: Mitigating the Rising Threat to Prominent People* is important because it occupies that more practical space. It is not a theoretical meditation on intelligence, nor is it a history of protective operations. It is a practitioner-focused book about how protective intelligence can be used to identify, understand, and mitigate threats before they become attacks.

That practical orientation is the book's central strength. Burton and Stewart are not writing as detached observers of the security profession. They write as practitioners who have spent decades examining threats, attacks, hostile actors, surveillance, targeted violence, and the operational realities of protecting prominent people. The result is a book that feels grounded in the world security professionals actually inhabit, one with imperfect information, unstable threat actors, behavioral indicators, public exposure, family vulnerabilities, travel patterns, residential security concerns, and the persistent difficulty of convincing busy or resistant principals to take security seriously before a crisis occurs.

The book is especially effective because it relies heavily on case studies. This is not a minor stylistic choice. In protective intelligence, case studies are often one of the most useful ways to teach professional judgment. Threats to prominent people are rarely clean, linear, or obvious in real time. Warning signs may exist, but they are often dispersed across behavior, communications, grievances, fixation, surveillance, access opportunities, and environmental vulnerability. A purely theoretical framework can describe these factors, but a case study can show how they converge. Burton and Stewart use cases to draw out practical lessons about pre-incident indicators, protective failures, attacker behavior, and opportunities for intervention.

This makes the book particularly valuable for the practitioner's bookshelf. Many security professionals do not need another abstract account of why intelligence is important. They need concrete examples of what protective intelligence looks like when applied to real threats against real people. They need to understand how hostile actors think, how grievances develop, how surveillance manifests, how routines create vulnerability, and how small failures in awareness can become significant openings for attack. Burton and Stewart's use of case studies helps translate protective intelligence from a concept into a professional practice.

The book also succeeds because it treats protection as something that begins well before the moment of physical confrontation. This is one of the most important distinctions between executive protection as a visible security function and protective intelligence as a preventive discipline. The public often imagines protection in terms of agents, vehicles, movements, and immediate response. Those functions matter, but they represent only one layer of a sound protection program. The deeper work begins earlier by identifying threats, assessing intent and capability, understanding exposure, detecting surveillance, reducing predictable patterns, and shaping behavior before the adversary has an opportunity to act. Burton and Stewart's argument is powerful because it places intelligence at the front end of protection rather than treating it as a supporting function after danger has already become apparent.

For executive protection professionals, this is a necessary corrective. Protective operations can become overly focused on proximity, logistics, and movement. Those skills remain essential, but they are insufficient if they are not informed by intelligence. A protection team that does not understand the threat environment is reactive by design. It may move well, drive well, and respond well, but it is still waiting for danger to reveal itself. Protective intelligence changes that posture. It allows the security program to think ahead of the attack cycle, to identify hostile interest before it becomes hostile action, and to shape the protectee's environment in ways that reduce opportunity.

The book is also useful because it recognizes that the threat to prominent people has changed. Prominence itself has become easier to create, easier to identify, and easier to target. Executives, public figures, wealthy families, media personalities, activists, academics, and other visible individuals now live in an environment where personal information can be collected, shared, and weaponized at speed. Doxxing, grievance communities, social media amplification, ideological polarization, copycat behavior, and public anger toward institutions all contribute to a more complex threat landscape. Due to this, protective intelligence is progressively more relevant to corporate leaders, high-net-worth families, controversial public figures, and others whose visibility makes them potential targets.

Burton and Stewart are at their best when they emphasize that security is not something done to a principal by a protection team. It is also something the principal and family must participate in through behavior, awareness, and discipline. This point is professionally important because many protective failures emerge from ordinary habits rather than dramatic lapses. Predictable routines, public schedules, exposed residences, casual social media use, unnecessary disclosure of travel, and resistance to basic protective measures can create vulnerability regardless of how competent the security team may be. The book's practical value is in its insistence that protective intelligence-led security requires participation from the people being protected.

This is also why the book should be read beyond the traditional executive protection community. Security managers, corporate security directors, threat assessment professionals, protective intelligence analysts, family office advisors, and even principals themselves can benefit from its approach. The book provides a bridge between the operational world of protection and the analytical world of threat assessment. It helps explain why protective intelligence is not a luxury or an abstract best practice, but a necessary function in any serious program responsible for prominent people.

The book's practitioner focus also raises a larger point about the development of the security profession. Security has no shortage of experience, but much of that experience remains difficult to transmit. Lessons are often passed through mentorship, after-action discussions, training courses, and informal professional networks. Those methods are valuable, but they can also be uneven. One of the reasons books like *The Protective Intelligence Advantage* matter is that they help convert practitioner experience into a more

durable body of professional knowledge. They preserve lessons that might otherwise remain confined to a particular agency, company, team, or generation of practitioners.

This is especially important in protective intelligence because the discipline depends so heavily on judgment. Technical tools can assist with monitoring, data aggregation, and investigative research, but they cannot replace the human capacity to interpret behavior, assess credibility, understand context, and distinguish between noise and warning. Case-based practitioner literature helps develop that judgment. It allows readers to examine past incidents, identify patterns, test assumptions, and think through how they might have recognized or mitigated the threat earlier. In this respect, the book does more than explain protective intelligence. It helps train the reader to think like a protective intelligence practitioner.

There are, of course, limits to what any single book can accomplish. *The Protective Intelligence Advantage* should not be mistaken for a comprehensive technical manual on every aspect of executive protection, threat assessment, residential security, or behavioral analysis. Readers seeking exhaustive methodological detail on any one of those subjects will need to supplement it with more specialized works. Yet that is not a serious weakness. The value of the book is found in its integration of experience, case studies, and practical principles. Its purpose is not to reduce protective intelligence to a checklist, but to demonstrate why intelligence-led security matters and how practitioners should think about the threat environment around prominent people.

For that reason, the book belongs on the practitioner's bookshelf. It is accessible enough for those newer to protective intelligence, but substantive enough to be useful to experienced professionals. It offers case studies without reducing them to entertainment, practical lessons without becoming simplistic, and professional judgment without excessive theorizing. Most importantly, it reinforces a principle that the security profession cannot afford to forget: protection is most effective when it begins before the attack.

In a field where too much knowledge remains fragmented, informal, or locked inside operational experience, Burton and Stewart have provided a useful contribution. *The Protective Intelligence Advantage* is valuable because it does something immediately useful, showing practitioners how to think about threats, how to learn from past attacks, and how to place intelligence at the center of protecting prominent people in an volatile security environment.

Book Review: Private Security: An Introduction to Principles and Practice by Charles P. Nemeth

The security profession possesses no shortage of expertise. Across the fields of executive protection, investigations, intelligence analysis, physical security, cybersecurity, crisis management, and resilience, practitioners have developed increasingly sophisticated methodologies for managing risk in complex environments. Despite this growth, one challenge remains persistent: security often lacks a shared intellectual foundation. Practitioners frequently enter the profession through highly specialized pathways and develop deep expertise within their chosen disciplines, but comparatively few opportunities exist to understand how those disciplines relate to one another within the broader enterprise of security management. It is within this context that Charles Nemeth's *Private Security: An Introduction to Principles and Practice* demonstrates its greatest value.

At nearly one thousand pages, the book is not designed to be a technical manual. Readers seeking detailed instruction on protective intelligence, investigations, physical security design, or cybersecurity will find more specialized texts elsewhere. Nemeth instead undertakes the more ambitious task of surveying the private security profession in its entirety. The result is less a handbook than a reference work; less a guide to performing security functions than an explanation of the profession itself. This distinction is critical because it speaks directly to a need that remains underserved within the security literature.

Most security professionals develop through a combination of operational experience, mentorship, certifications, and training programs. These pathways are invaluable, but they also tend to be highly specialized. Executive protection professionals learn protective operations. Investigators learn investigative methodologies. Intelligence analysts learn collection and analytical techniques. Security managers learn administration and program oversight. While these educational pathways produce capable specialists, they do not necessarily produce a common understanding of the profession as a whole. As a result, many practitioners possess exceptional knowledge within their area of expertise while remaining comparatively unfamiliar with adjacent disciplines that increasingly influence their work.

This challenge has become more pronounced as the security profession has evolved. The distinctions that once separated physical security, intelligence, investigations, executive protection, cybersecurity, and business continuity have become progressively blurred. Modern security risks rarely respect organizational boundaries. A workplace violence case may involve protective intelligence, investigations, access control systems, executive protection concerns, crisis communications, and legal considerations simultaneously. Likewise, a corporate security director may be expected to oversee functions spanning multiple specialties despite having entered the profession through only one of them. Because of this, the contemporary security environment demands breadth in addition to depth.

It is here that Nemeth's work makes its most significant contribution. Rather than focusing narrowly on operational techniques, the book provides readers with a conceptual framework through which the various components of private security can be understood as part of a larger profession. Topics ranging from legal authorities and investigations to critical infrastructure protection and information security are

presented as interconnected elements of risk management. The value of this approach lies not in the technical detail of any individual chapter, but in the cumulative effect of seeing the profession as a coherent whole.

Indeed, some readers may criticize the book precisely because of its breadth. No single volume can provide equal depth across the entirety of private security. Specialists will inevitably encounter sections that cover familiar territory at a level they consider introductory. Such criticism, while understandable, risks misunderstanding the purpose of the work. The book is not attempting to produce experts. It is attempting to produce perspective. In that respect, breadth is not a weakness but a deliberate design choice.

This raises a broader question about the development of the security profession itself. Mature professions are distinguished by the existence of a shared body of knowledge. Lawyers, physicians, engineers, and political scientists possess foundational texts that help define the boundaries, concepts, and assumptions of their respective disciplines. Students entering those professions are expected to understand not only their specialization but also the larger intellectual framework within which that specialization operates. Security has historically lagged behind in this regard. Much of its knowledge has remained distributed across certifications, vendor training, operational experience, and specialized publications. While these resources contribute significantly to professional competence, they do not always provide a comprehensive understanding of the profession itself.

Works such as Nemeth's help address this deficiency. They serve an important professional function by creating a common vocabulary and intellectual foundation that can be shared across specialties. This function is particularly important at a time when security organizations increasingly seek integrated approaches to risk management. Effective collaboration between investigators, intelligence analysts, executive protection professionals, cybersecurity specialists, and security managers requires more than technical competence. It requires a shared understanding of the broader mission and the interdependence of their respective disciplines.

For this reason, the greatest value of *Private Security: An Introduction to Principles and Practice* may not sit in any individual chapter. Its significance exists in its effort to define and explain the profession itself. In doing so, Nemeth provides students with a roadmap, managers with a reference, and experienced practitioners with an opportunity to view their specialty within the larger context of modern security practice.

As private security continues to expand in scope, responsibility, and complexity, the profession will require more works of this kind, not fewer. The future of security will undoubtedly depend upon specialized expertise. It will also depend upon practitioners who understand how those specialties fit together. Nemeth's book represents a meaningful contribution toward that goal and serves as a reminder that professions are built not only through practice, but also through the development of a shared body of knowledge.

Submitting to the Journal

The Close Protection and Security Journal is a bi-annual publication, and we welcome submissions from scholars, researchers, and practitioners on a number of topics. The scope of the Journal is intentionally broad as there are currently no scholarly publications dedicated only to corporate security. Importantly, the intention of the Journal is to be a scholarly publication led by practitioners, offering their in-depth insights into historic cases, current issues, and emerging threats. The Journal aims to publish articles by authors who have professional or academic research experience with the subjects of their writing to better give insight into corporate security. Professional experience from prior military or government service is also acceptable as a means to bring important ideas from related fields to corporate security.

Topics for the Journal include but are not limited to:

- Close Protection
- Red Teaming
- Security Failures
- Intelligence Analysis
- OSINT
- Emerging Technology
- Due Diligence
- Event Risk Management
- Enterprise Risk Management
- Security Operations Centers
- Political Risk
- Skill Development for Security
- Surveillance/Counter-Surveillance
- Private Security History

Submission Instructions

Please submit your articles to the Editor-in-Chief Dr. Treston Wheat at treston.wheat@ips-board.org as a .doc or .docx attachment by the deadline. Include a short biography about yourself to describe your qualifications to write on the subject of your article.

Please contact Dr. Wheat or members of the editorial board with any questions that you might have regarding journal submission or content.