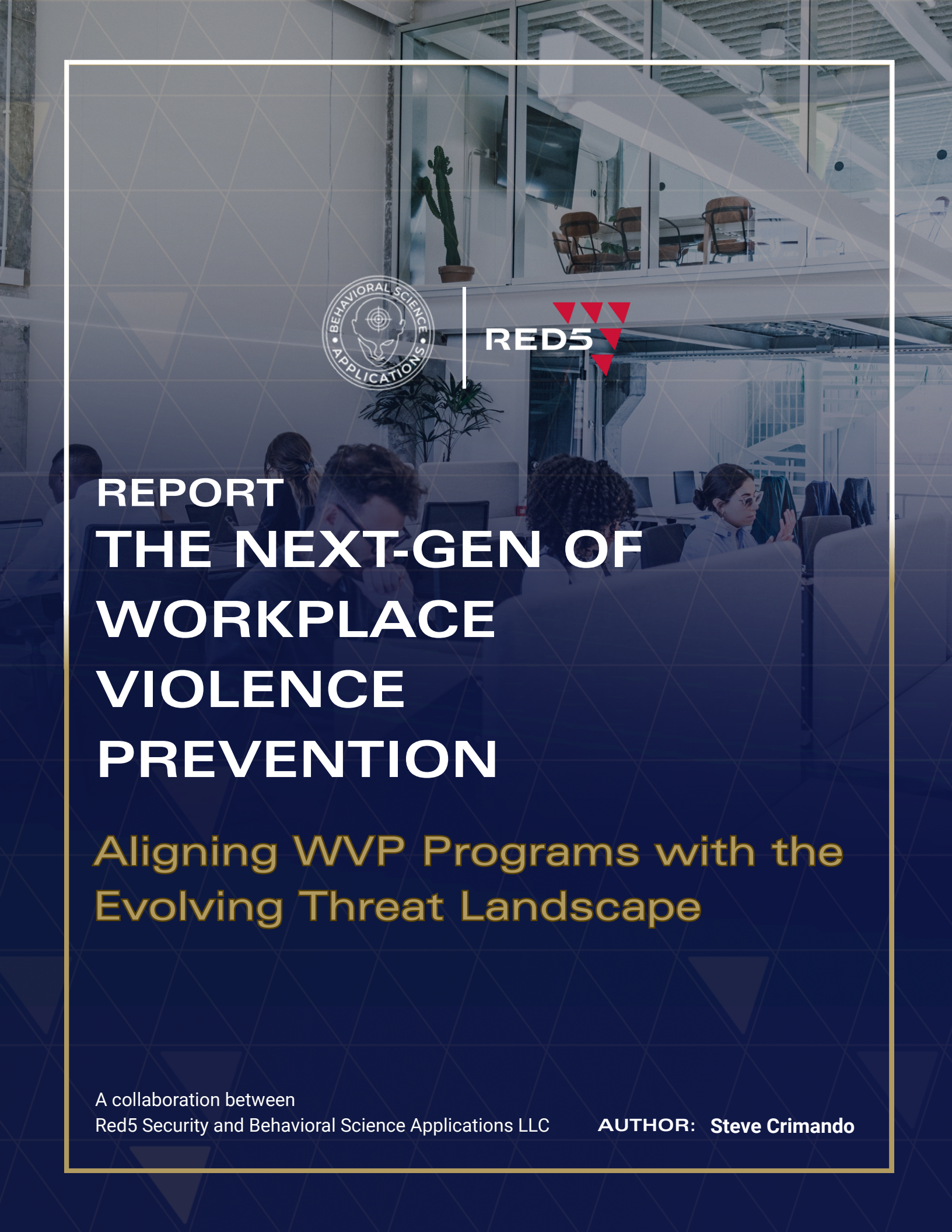


REPORT

THE NEXT-GEN OF WORKPLACE VIOLENCE PREVENTION

Aligning WVP Programs with the Evolving Threat Landscape

A collaboration between
Red5 Security and Behavioral Science Applications LLC

AUTHOR: **Steve Crimando**

Ideological Risk and the New Corporate Threat Landscape

In an era of unprecedented social fragmentation, the "corporate perimeter" is no longer defined merely by office walls or firewalls, but by the volatile ideologies of a polarized public.

Businesses and their executives are increasingly finding themselves caught in the crosshairs of an ideological violence shift driven by a toxic mix of extreme political polarization, the weaponization of social media, and a "new normal" where corporate policy is viewed as a partisan battleground.

What was once the domain of distant geopolitical risk has moved into the local boardroom; today, a CEO's public statement or a company's ESG commitment can trigger not just a PR crisis, but credible physical threats and targeted sabotage.

Corporate leaders are facing a heightened threat environment driven by social polarization and extreme ideologies.

Over the past few years there has been a significant and documented increase in threats to CEOs involving both physical violence and digital attacks resulting in increased executive protection spending reflecting heightened concerns around:

Personal risk

Activism

Geopolitical Instability

Numerous CEOs of major tech firms have had their home addresses and private travel schedules leaked ("doxxing"), leading to "swatting" incidents where emergency services are falsely called to their homes to provoke a high-stakes police response.

For modern leadership, safeguarding the enterprise and key leadership personnel now requires a sophisticated understanding of how social grievances can rapidly escalate into operational disruptions, making ideological risk management an essential pillar of 21st-century corporate security and resilience.

From a Duty of Care perspective, workplace violence prevention is a legal and ethical obligation for employers to take all reasonable steps to ensure the safety, health, and well-being of their employees.

Everyone in a leadership role, including professionals working corporate security and executive protection, as well as HR and legal roles, must recognize that violence against an organization or its executives may be considered foreseeable, especially in high-risk sectors. Foreseeability generally falls into two categories that determine an organization's Duty of Care:

General Foreseeability: Is the type of harm predictable based on the nature of the business? For example, a company in a controversial industry (e.g., energy, pharmaceuticals, or defense) may have a higher baseline of foreseeability for ideological protests or attacks.	**Specific Foreseeability:** Is there a specific threat against a specific executive or facility? This is triggered by direct communications, social media manifestos, or a history of "near-miss" incidents involving a particular group.

When dealing with ideologically motivated threats—such as those stemming from political, social, or extremist causes—the standard for what a company "should have known" becomes more complex and challenging as a potential liability.

In the current environment, expanding the traditional framework for workplace violence prevention is no longer just a theoretical exercise; it is a pragmatic necessity.

For decades, the Occupational Safety and Health Administration (OSHA) has relied on a four-part typology to categorize workplace violence, ranging from random criminal acts to personal vendettas. However, as the line between social activism and violent extremism blurs, a fifth category is emerging.

The Evolution of Workplace Violence: OSHA's Traditional Typology

Since 1996, the Occupational Safety and Health Administration (OSHA) has categorized workplace violence into four distinct types based on the relationship between the perpetrator and the organization. Understanding these categories is the first step in developing a targeted risk-mitigation strategy.

Type I: Acts of Criminal Intent The perpetrator has no legitimate relationship with the business or its employees. The primary motive is usually theft, robbery, or trespassing, and the violence is incidental to the underlying crime.	**Type II: Customer/Client Violence** This typically involves a "legitimate" user of the business—such as a patient, student, or customer—who becomes violent during the delivery of routine services.
Type III: Worker-on-Worker Arising from internal conflicts, where a current or former employee, supervisor, or manager targets coworkers or leadership, typically due to interpersonal disputes or professional grievances.	**Type IV: Personal Relationship Violence** Occurs when an intimate partner or domestic abuser follows an employee to work, transforming the workplace into a secondary battleground for personal conflicts.

The Threat Environment is Evolving

While these four categories have served as the industry standard, they focus heavily on transactional or interpersonal motives. The emergence of possible "Type V" workplace violence signals a shift toward symbolic motives—where the perpetrator views the entire organization through an ideological lens rather than a personal or financial one.

Violence can be directed by an individual or group at an organization, its leadership and assets because of what the organization does or represents.

While no sector is entirely immune, certain industries face heightened risks due to their symbolic value, their role in critical infrastructure, or their involvement in polarizing social issues.

Sectors with elevated levels of concern include:

Technology and Artificial Intelligence:
A notable trend in 2026 is the rise of anti-tech and anti-AI sentiment.

- **Data Centers and AI Infrastructure:** As AI becomes more integrated into daily life, it has drawn the ire of nihilist and "neo-Luddite" extremist subcultures who view the technology as an existential threat to humanity or employment.
- **Telecommunications:** 5G infrastructure continues to be targeted by conspiracy-driven actors who link the technology to various health or surveillance theories.

Energy and Critical Infrastructure:
This sector is a primary target for "accelerationist" ideologies—groups that seek to trigger societal collapse by disabling vital services.

- **Electric Power Grid:** Substations and transmission lines are high-priority targets due to their vulnerability and the cascading impact of a blackout.
- **Water and Oil/Gas:** These remain "soft targets" where physical sabotage can cause significant economic and public health disruption.

Healthcare, Reproductive Services, and Life Sciences:
Healthcare continues to be a flashpoint for ideological violence, particularly in areas tied to social and biological ethics.

- **Reproductive Health Clinics:** Historically a target of anti-abortion extremism, these facilities remain at high risk.
- **Gender-Affirming Care Providers:** Emerging ideological shifts have increasingly placed LGBTQ+ healthcare providers in the crosshairs of far-right extremist rhetoric.
- **Life-Science/Pharmaceutical:** Grievances over drug pricing, vaccine mandates, or clinical trial outcomes.

Retail and "Soft Targets":

- Public-facing businesses are often targeted not because of what they do, but because of who gathers there.
- Retailers have also been targeted by activists because of their DEI positions or endorsements of controversial social issues or personalities.

Public Sector and Governance: The "militarization of political disagreement" has turned routine government operations into high-risk environments.

- **Election Infrastructure:** Workers and polling sites face threats from those who believe in election-related conspiracy theories.
- **Education (K-12 and Higher Ed):** Schools and universities have become battlegrounds for "culture war" issues, leading to threats against school boards and DEI (Diversity, Equity, and Inclusion) programs.

Dominion Voting Systems Executives
Following the 2020 U.S. election, several executives, including Eric Coomer, were forced into hiding due to a relentless barrage of death threats and physical stalking by individuals motivated by election-related conspiracy theories.

Shopping Malls and Entertainment Venues:

- These are perceived “soft targets” for mass-casualty attacks by threat actors seeking high-visibility impact.

Faith-Based Organizations:

- Synagogues, mosques, and churches remain top targets for hate-motivated violence driven by antisemitic, Islamophobic, or white supremacist ideologies.

In addition to certain sectors having greater risks of ideological violence, the actions of executives and other high-profile employees can attract the ire of radicalized true believers.

Executives who have been vocal about or associated with controversial political figures or initiatives through endorsements, appearances or donations, can find themselves targeted by activities and extremists.

Ideologically inspired individuals and groups may target an organization or its leaders to stop perceived harm, to make a statement or to intimidate others working certain sectors and industries.

A Fifth Type of Workplace Violence?

The U.S. Occupational Safety and Health Administration (OSHA) defines workplace violence as any act or threat of violence against workers while they are at a worksite or on duty.

According to OSHA, workplace violence can occur at any location where work-related functions are conducted, including:

- **Physical Workplace**
- **Off-Site Meetings**
- **Company Vehicles**
- **Employees' Homes During Work-Related Activities**

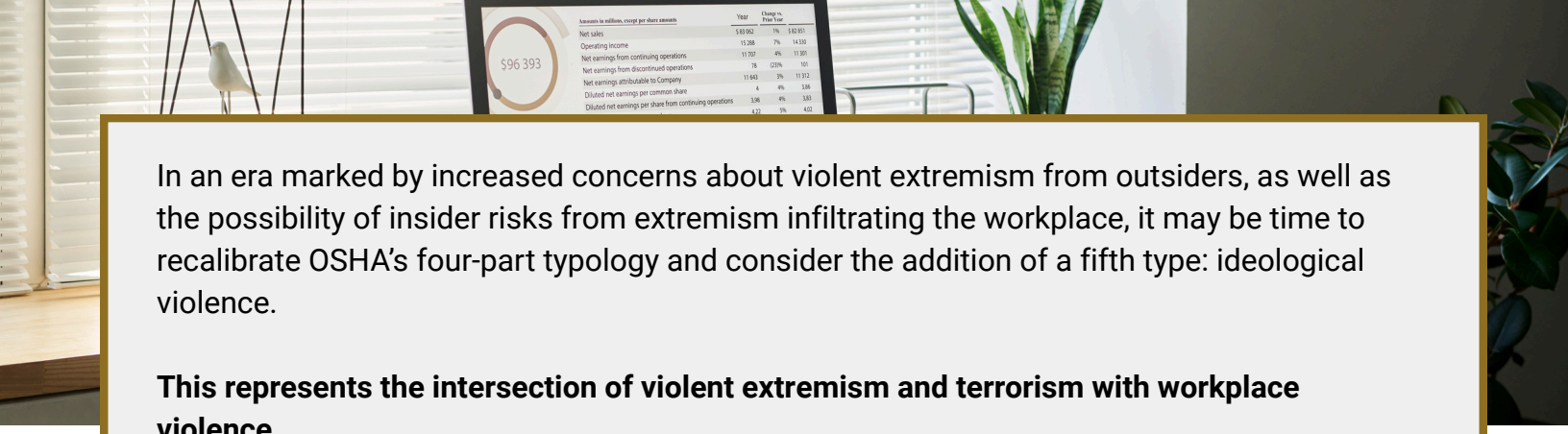
Highsmith, Carol M., 1946-, photographer | picryl

The suspect in the targeted attack on UnitedHealthcare CEO Brian Thompson was initially charged by the Manhattan district attorney with killing as an act of terrorism.

District Attorney Alvin Bragg labeled the incident as "a frightening, well-planned, targeted murder" aimed at causing shock and intimidation. The suspect's writings reveal a focus on Thompson, criticizing the healthcare insurance industry and high executive pay linked to denying medical care.

In the UnitedHealthcare case referenced above, Mr. Thompson was clearly "on duty," traveling to an investor conference to represent his employer. On the day of the attack, the off-site meeting was his "workplace."

This event highlights the need for comprehensive safety measures and policies that protect employees, regardless of where they may be performing their job duties. As the lines between personal and professional spaces blur, it becomes imperative to adapt the approaches to workplace safety to encompass these new realities.



In an era marked by increased concerns about violent extremism from outsiders, as well as the possibility of insider risks from extremism infiltrating the workplace, it may be time to recalibrate OSHA's four-part typology and consider the addition of a fifth type: ideological violence.

This represents the intersection of violent extremism and terrorism with workplace violence.

Type V workplace violence can be defined as violence directed at an organization, its people, or its properties for ideological, religious, or political reasons. Consider these notable examples:

- The April 2026 arson attack at the Kimberly-Clark distribution center in Ontario, California, by an employee who had posted videos to social media alongside a manifesto-style anti-capitalist rant comparing himself to Luigi Mangione
- The April 2026 Molotov cocktail attack on the home Open AI's CEO's home and attempted attack at corporate headquarters by an anti-AI extremist who was arrested carrying a firearm and manifesto with a hit list of AI executives.
- The attacks on political figures and their spouses at their homes in Michigan leaving two dead and two seriously injured.
- The Unabomber's 1994 killing of a senior advertising and PR executive at his home in New Jersey. The executive was targeted because of his firm's efforts to rehabilitate Exxon's reputation following the Valdez oil spill.
- Two brothers associated with al Qaeda carried out a 2015 massacre of the editorial staff at the Paris offices of Charlie Hebdo—as retaliation for the satirical magazine's attacks on political and religious leaders.
- A violent men's rights extremist's 2020 attack on the New Jersey home of U.S. District Judge Esther Salas. The attack killed her son and wounded her husband.

Each of these incidents are examples of targeted violence based on ideological grievances tied to the victims' professional roles and activities.

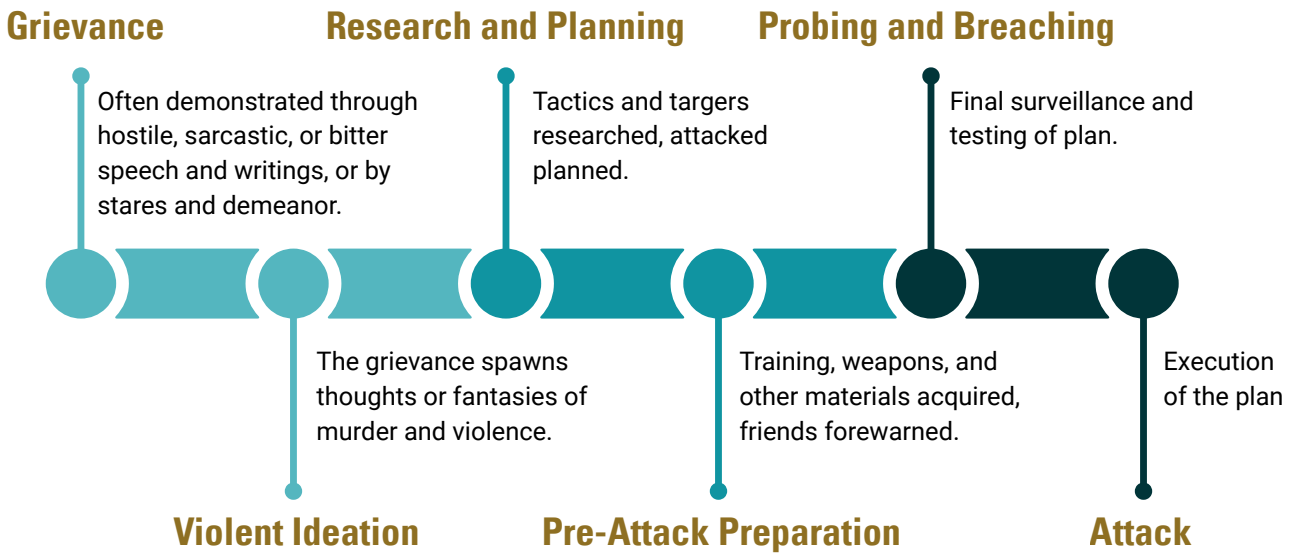
This, of course, includes the December 2024 killing of United Healthcare's CEO, allegedly committed by an extremist whose manifesto focused on "parasitic" and "too powerful" corporations for "abusing our country."

The Benefits of Expanding the Model

Ideological violence — whether perpetrated by lone actors or recognized groups—remains a persistent threat to organizations and their personnel. Notably, businesses were the most frequent targets of U.S. terrorist attacks between 1970 and 2020.

Workplace violence prevention programs can be matured and better aligned with the evolving threat landscape through the addition of ideological violence as a fifth element expanding OSHA's existing typology. By doing so, organizations may be able to further leverage the workforce and other resources for violence prevention and executive protection.

Workplace violence prevention relies heavily on others in contact with a person or group of concern to recognize and report behaviors and communications indicative of potential movement along a pathway to intended violence.



The Pathway to Violence model pioneered by researchers Calhoun and Weston in 2003 has since been adopted by the U.S Department of Homeland Security. It distinguishes predatory (targeted) violence—which is planned, cold-blooded, and methodical—from affective (reactive) violence, which is impulsive and driven by heat-of-the-moment emotion.

Targeted violence doesn't happen in a vacuum; it is an evolutionary process where the attacker moves from violent thoughts to violent actions through a series of identifiable steps.

Research from the FBI and U.S. Secret Services indicate that there are typically pre-incident indicators that suggest that someone might be progressing towards a violent resolution to their perceived grievance.

In typical workplace violence scenarios, common grievances include:

- adverse interpersonal actions
- employment or financial actions against an attacker
- increased stressors such as personal or professional relationship problems.

In ideological violence directed at organizations, grievance is less likely to be related to the perception of personal harm than advancing or defending a particular belief or cause.

A common element in most workplace violence prevention training programs is the emphasis on co-workers recognizing and reporting concerning behaviors that may be indicative of violence risk.

Such pre-incident risk indicators include behaviors and communications associated with workplace violence, such as sudden or dramatic changes in an employee's behavior or appearance, a loss of emotional or physical control, and threats or acts of violence.

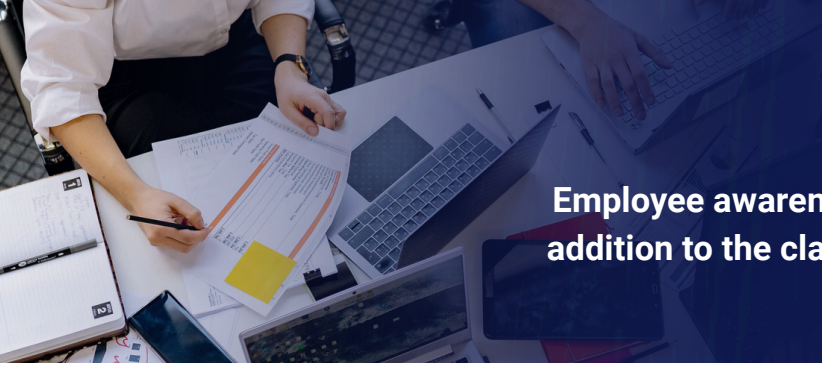
The behavioral indicators associated with the OSHA's four types of workplace violence are substantially different than the indicators of ideological violence and instead are more consistent with the warning signs of terrorism such as:

Hostile Surveillance

Elicitation

Tests of Security

Attempted Intrusion



Employee awareness of the signs of ideological violence in addition to the classic four types of workplace violence can create a force-multiplier effect.

For example, warning behaviors associated with targeted violence, such as fixation or leakage, may signal extremist activity in a coworker, vendor, customer or community member.

Employees can and should be empowered to recognize behaviors and communications related to any form of violence, including ideological violence.

As such, blending awareness of the risk indicators of ideological violence into programs addressing traditional workplace violence concerns creates more sensors; more eyes and ears are more likely to recognize behaviors and communications as potential risk indicators.

Warning Behaviors Associated with Ideological Violence

Leakage: Communication to a third party of an intent to do harm to a target.

Fixation: An increasing negative preoccupation with a person, cause, or previous attackers.

Identification: Adopting the "warrior" persona associated with a specific belief or a cause.

Addressing ideological violence directed at organizations and their leaders as something other than workplace violence creates a false dichotomy.

Regardless of the motive, violence directed at an organization, its leaders, workforce and properties is targeted violence; it is premeditated and purposeful. Violence of this type is a process, not a singular event, and the process can be disrupted to mitigate the risk.

Mitigation of ideological threats is best addressed by empowering employee recognition and reporting, along with enhanced security intelligence, and threat monitoring.

Leakage, communication to a third party of an intent to do harm is the most common behavioral risk indicator. Unlike a direct threat made to the victim, leakage is often overheard by peers, posted on social media, or in virtual communities.

Open Source Intelligence (OSINT) and active threat monitoring are therefore essential elements of ideological violence prevention.

Threat Intelligence (TI), the collection, processing, and analysis of data to understand an adversary's motives, targets, and attack behaviors, can help inform corporate security, travel security and executive protection, shifting from a reactive stance to a proactive stance.

Foreseeability to this risk begins with the assessment of an organization’s exposure to Type V workplace violence. This can be structured as a simple four-part survey.

Operational Exposure

How the business interacts with the public can create friction points.

- **Event Hosting:** Does the business host town halls, political rallies, or high-security speaking engagements?
- **Supply Chain & Partnerships:** Are any of the business' partners or vendors currently the target of active boycotts or extremist campaigns?
- **Product/Service Impact:** Does the core service of the company inherently conflict with a specific extremist ideology (e.g., animal research, fossil fuel extraction, or diverse representation in media)?

Digital & Information Footprint

In the modern era, Type V violence often begins with "doxxing" or online radicalization.

- **Sentiment Analysis:** What is the current "temperature" of the organization’s mentions on fringe platforms (e.g., 4chan, Telegram, or specialized extremist forums)?
- **Data Security:** How easily can an outsider find the home addresses, personal phone numbers, or daily routines of key employees?
- **Information Leakage:** Has there been an uptick in unusual information-gathering requests (FOIA requests, aggressive social engineering, or suspicious photography of the premises)?

Recalibrating the Approach to Workplace Violence Prevention

The current social and political climate calls for modernizing and maturing existing workplace violence prevention policies and plans, as well as employee awareness training programs to include discussion of Type V violence, along with the associated risk indicators and instructions on how to report concerns.

As with other forms of workplace violence, employees are the essential "human sensors" of an organization. While cameras and badge readers track movement, only people can track intent and vibe.

Detection and defense against Type V workplace violence requires a blend of “hard” measures, such as security technologies with employee intuition as a "soft" intelligence network.

Enabling employees to effectively identify this type of risk requires both executive support for a strategic framework that recognizes ideologically motivated violence against the organization or its personnel as workplace violence, and employee awareness of the associated behaviors.

Traditional workplace violence training focuses heavily on Type III, worker-on-worker violence, and the concept of the “disgruntled” employee. The behavioral risk indicators of a progression towards that type of violence are completely different than those suggesting someone might be advancing along a pathway toward ideological violence

Indicator	Type III (Internal)	Type V (Extremist/Ideological)
Motivation	Personal grievance/adverse employment action	Political, social, or "moral" cause
Target	Specific supervisor or peer	The "Brand," the HQ, or a "Class" of people
Warning Sign	Withdrawal/anger/aggression	Surveillance/Ideological outbursts
Relationship	Current/Former Employee	Usually an Outsider/Stranger

In addition to efforts to educate the workforce about the behavioral risk indicators associated with Type V workplace violence, security professionals and others involved in the organization's violence prevention efforts can benefit from continuing education and threat awareness, as well as the development of critical relationships, by participating in public-private information sharing initiatives such as the Global SHIELD Network and InfraGard.

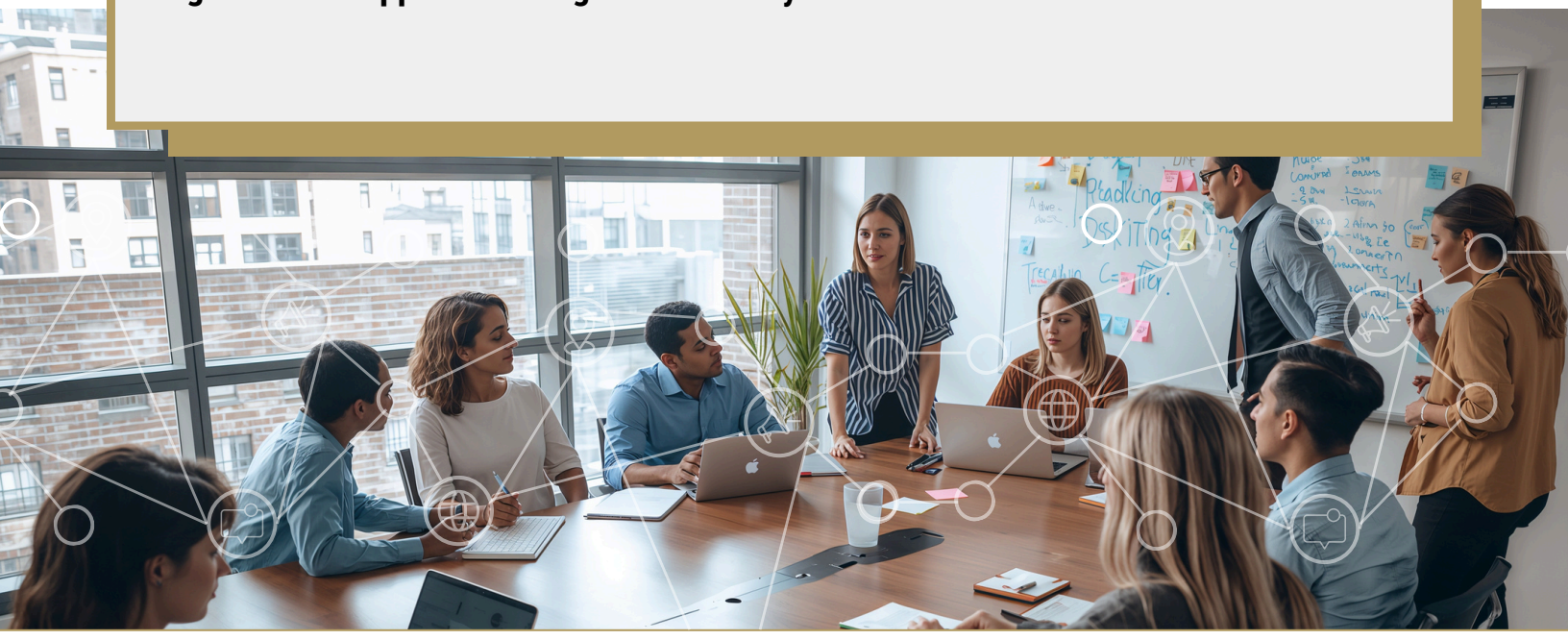
Involvement in these types of organizations help security and executive protection professionals stay informed of current trends and foster relationships for countering extremism or terrorism that may target businesses.

The nature of workplace violence is rapidly changing and increasingly includes the possibility of targeted violence directed at organizations and their key personnel in response to social issues or extreme ideologies.

Extremism in the workplace is becoming mainstream, and social and political divisions marked by angry rhetoric are more common.

Recent tragedies may be the catalyst for recalibrating existing models of workplace violence prevention to be better aligned with the evolving threat landscape.

It is time to revisit the topic of workplace violence prevention and ensure the organization's approach is aligned with today's risks.



About the Author

Steve Crimando is the founder and principal of Behavioral Science Applications LLC. He is an emergency behavioral health clinician, educator, and crisis responder with nearly four decades of experience in threat assessment and violence prevention.

Steve is a Certified Threat Manager (CTM) with the Association of Threat Assessment Professionals (ATAP) and a Certified Master Trainer for the U.S. Department of Homeland Security National Threat Evaluation and Reporting (NTER) program.

He is a cleared mental health partner to the FBI Joint Terrorism Task Force (JTTF), as well as an advisor and instructor for the FBI's Community Anit-Threats Officer (CATO) program.

Steve serves as the Chair of the Extremism & Political Instability Community (EPIC) Steering Committee and a member of the Human Threat Management Community Steering Committee for ASIS International.

He is a published author frequently called upon by the media and the courts as an expert in violence prevention and response.

Steve was deployed as a crisis responder to both the 1993 and 2001 World Trade Center attacks, the New Jersey's anthrax screening center and many other acts of mass violence. He has served as a mental health specialist on the Bergen County (NJ) Police Department Hostage Recovery Team (HRT), the New Jersey Police Surgeons Team, and the United Nations Office for Operational Support-Special Situations Unit.