Managing political violence and instability.



A Guide for Corporations

liferaft
A Securitas company

Table of Contents

Foreword 1

Executive Summary 2

Review Of Foundational Literature 4

Threat Environment: Political Violence & Instability in the U.S. 7

Political Actions vs. Expressions. 8

- Tier 1: Political Violence with Intent to Harm, Including Terrorism 9
- Tier 2: Unlawful Civil Disobedience, Property Destruction, & Similar Activity 11
- Tier 3: Lawful Activism & Demonstration. 12

Ideologies & Motivations 14

A Framework for Managing the Risk 15

- Phase 1: Organization Assessment 16
- Phase 2: Risk Assessment 18
- Phase 3: Mitigation 20
- Phase 4: Continuous Improvement 23

Summation 24

Resources You Can Use 25

Summation 25

About the Authors 26

How Liferaft Can Help 28

Foreword by Mark Freedman

When I served as a U.S. State Department officer, including as Chief of Staff to the Ambassador-at-Large for Counterterrorism, the terrorism threat facing the United States was serious but, in an important sense, legible. Al-Qaeda and ISIS were formidable adversaries, and countering them consumed significant national effort. But we largely understood who they were, what they wanted, and how they operated. Their ideologies were coherent, their organizational structures identifiable, and their targeting logic followed patterns we could study and anticipate. The threat was high, but it was also relatively clear.

> **Corporate security teams cannot manage what they cannot see.**

As threats from those international terrorist groups persist, the security environment facing us today is defined not by a single dominant adversary but by a diverse and shifting constellation of actors and motivations, both foreign and domestic. Grievances that once lived at the fringes now move quickly into the mainstream and the risk of political violence and instability in the United States has become more complex. Lone individuals may radicalize on timelines measured in weeks, drawing from an ideological menu they assemble themselves. Nation-state adversaries, ideological movements, single-issue extremists, and unaffiliated actors now occupy the same threat landscape, and the lines between them blur more each year.

Nowhere is this shift more consequential for the private sector than in the rise of anti-corporate extremism. The murder of UnitedHealthcare CEO Brian Thompson, the alleged attempt on the life of OpenAI's Sam Altman, and an alleged plot against a White House event whose target list included corporate executives are signals of a broader dynamic in which companies and their leaders are cast as antagonistic symbols and painted as legitimate targets. For those of us who have studied this field, it calls to mind the environmental and animal rights extremism of the Earth Liberation Front (ELF) and Animal Liberation Front (ALF) a generation ago, but faster-moving, more diffuse, and dramatically amplified by the online ecosystems where these ideas now germinate and spread.

This is a genuinely difficult environment for companies to understand and interpret, and it is harder still to know how to respond. Overreaction can carry real costs, in dollars, in employee trust, and in the reputational damage that comes from appearing to treat legitimate criticism as a threat. Underreaction can be catastrophic. And the two failure modes are not always easy to tell apart in the moment. Security leaders must weigh physical protection against reputation, distinguish protected expression from genuine warning signs, and make consequential judgments on incomplete information and compressed timelines.

Getting these judgments right depends on visibility, and that is where Liferaft is an essential part of the mix. So much of what drives modern political violence and instability now takes shape in the online forums and echo chambers where grievances harden into ideology and, in some cases, into intent to harm. Corporate security teams cannot manage what they cannot see. Liferaft gives them insight into precisely those spaces, surfacing the early signals that let organizations distinguish real risk from noise and act before a threat materializes.

It is in that spirit that Rebel Global Security and Liferaft partnered to develop this guide. Our aim is to give corporate security and intelligence teams a clear-eyed assessment of the political violence and instability threat as it stands in 2026, together with a practical, defensible framework for managing it. The threat environment will keep evolving, and no single document can be the last word. But my hope is that this guide helps security and intelligence practitioners make sense of a complicated moment and provides some assistance in protecting their people, their organizations, and their social trust.



Mark Freedman
Principal and CEO, Rebel Global Security

SECTION 02

Executive summary.

This guide is intended to serve as a foundational resource for corporate security and intelligence teams working to understand and manage the risk of political violence and instability to their organizations. Specifically, it includes a novel framework designed specifically for security intelligence teams to help them assess risks, mitigate them, and continually improve in the face of mounting political instability.

This guide responds to a threat environment in the United States that has changed markedly in recent years: one defined by rising political polarization, a documented increase in domestic terrorism and targeted violence, and a series of high-profile attacks and plots against corporate leaders. More importantly, this guide fills a gap in the literature, which is robust in its treatment of the terrorism threat and governmental responses but light in practical guidance for corporations. As the 2026 midterm elections approach, corporations face yet another political inflection point that may raise the risks facing their people, property, operations, and reputation.

The guide begins with a review of foundational frameworks and literature. Together, these sources form the foundation upon which the guide's recommended framework is built. Key sources reviewed include:

GOVERNMENT

ISC Risk Management Process Standard

The Department of Homeland Security's (DHS) Interagency Security Committee (ISC) Risk Management Process Standard, which provides a five-step risk management methodology designed for protecting federal facilities from terrorism, and which can be adapted to a private sector context.

INDUSTRY

ASIS ESRM Guideline

The ASIS Enterprise Security Risk Management (ESRM) Guideline, which places security risk in a business context, helping security teams link threats to enterprise impact.

ACADEMIC

The Two-Pyramids Model

The Two-Pyramids Model of political radicalization from academics Clark McCauley and Sophia Moskalenko, which provides a heuristic for distinguishing the radicalization of opinion from the radicalization of action, a key insight that is especially critical for corporate security teams facing today's complex risk environment.

This guide then provides an analysis of the political violence and instability threat environment in the United States as of the time of writing. Our analysis examines these risks across tiers of differing severity. These tiers include political violence with intent to harm, including terrorism; unlawful civil disobedience, property destruction, and similar activity; and lawful activism and demonstration. For each tier, we distinguish between political actions and expressions (e.g., a social media post supporting terrorism as opposed to a terrorist act itself), since the risk posed and the appropriate response to each differ.

TIER 1 Political violence with intent to harm, including terrorism

TIER 2 Unlawful civil disobedience, property destruction, and similar activity

TIER 3 Lawful activism and demonstration

Executive summary.

The threat analysis explores a political environment in the United States in which political activity, across a spectrum from legal and peaceful to illicit and violent, is becoming increasingly volatile and unpredictable. Long-standing ideologies and motivations, including far-right, far-left, Islamist, and single-issue persist, even as a growing number of lone actors pick and choose from seemingly antithetical belief systems to justify their violence.

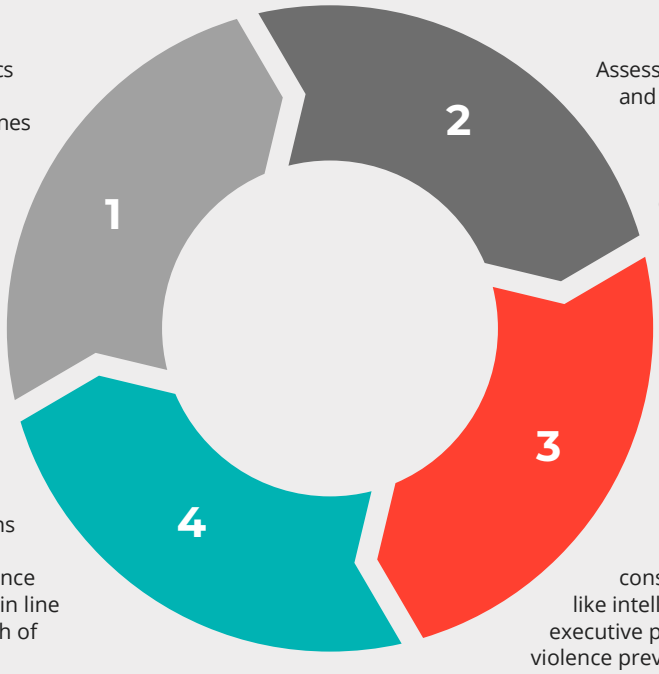
Our analysis also underscores that while it is critically important for security intelligence teams to endeavor to distinguish between political expressions and actions, the two are not always independent. Rhetoric can incite action, and a marked uptick in heated online chatter may precede activities and disruptions in the real world. Interpreting the narrow lines between protected expression, genuine warning signs, and incitement is one of the most difficult tasks a security team has in this environment.

The heart of this guide is a novel four-phase framework for managing the risk of political violence and instability, built specifically for corporate security and intelligence teams. The framework, which takes the form of a cycle, walks security teams through an ongoing risk management process that includes the following four steps:

Risk Management Process

Organization Assessment

Evaluate the company's key characteristics in the context of political violence and instability. Here, the security team examines their company's industry, symbolic value, geography, scale, and notable executives to understand whether, why, and to whom the organization is an attractive target for political violence or other political actions.



Risk Assessment

Assess the type and nature of political violence and instability threats the organization faces both directly and indirectly. The security team assesses political expressions and actions, including their legality; distinguishes between security risks and reputational risks; and develops liaison relationships that can deepen their intelligence picture.

Continuous Improvement

Improve efforts to manage political violence and instability risk as conditions evolve. The security team ensures that efforts to manage risks of political violence and instability are continually matured in line with the threat environment and growth of the business.

Mitigation

Select and integrate mitigation measures to address political violence and instability risk. The security team considers how corporate security functions like intelligence, physical security, cybersecurity, executive protection, insider threat and workplace violence prevention can be strengthened to address political violence and instability specifically.

The guide concludes with a summation and a list of resources that can be used to support implementation of the framework. In particular, security intelligence teams are encouraged to make regular use of the publicly available databases and other resources on political violence and terrorism listed at the end of this document. These resources will help practitioners better understand the contours of political violence, how terrorist and extremist movements have evolved in the past, and what risk they may pose in the future.

SECTION 03

Review of foundational literature.

This guide provides a novel framework that corporate security and intelligence teams can use to manage the risk of political violence and instability to their organizations. When developing this framework, we wanted something that would be easily applied by corporate security teams but also something familiar and defensible, grounded in the large body of existing standards, guidelines, and academic literature related to security and terrorism.

This section provides an overview of relevant standards and guidelines, from government and industry, as well as academic literature, which we believe are particularly relevant to how corporations should manage the risk of political violence and instability in 2026 and in the coming years.

Interagency Security Committee Standard: The Risk Management Process: Access Here

5 Steps to the ISC Risk Management Process

The Interagency Security Committee (ISC), a U.S. government body chaired by the U.S. Department of Homeland Security (DHS), was established in the wake of the 1995 Oklahoma City bombing, which remains to this day the deadliest act of domestic terrorism in American history.

One of the ISC's foundational guidance documents is the ISC Risk Management Process Standard, which lays out a five-step methodology for securing federal government facilities in the United States from terrorism and other physical security threats. The five steps are:

1. **Determine the Facility Security Level and Baseline Level of Protection:** What level of security should a given facility have, and what countermeasures are associated with that?
2. **Identify and Assess Risk:** Does a particular facility face higher or lower risks than the baseline, and how should countermeasures be adapted to match?
3. **Develop Risk Management Strategy:** What is needed to achieve the level of protection indicated for a given facility?
4. **Implement Risk Management Strategy:** What is the process for implementing and documenting countermeasures?
5. **Measure Performance:** Is everything functioning as intended, and what needs to be improved?

Although developed for federal use, the Standard's methodology is broadly applicable and should be known to all security practitioners seeking to mitigate the risk of terrorism, political violence, and instability to their organizations. Beyond the Standard, the ISC also publishes several other best practices, guidance documents, and white papers that can be helpful to corporate security teams. Topics include active shooter mitigation, making a business case for security, and protecting against the threat of unmanned aerial systems (UAS).

Source: Interagency Security Committee, The Risk Management Process: An Interagency Security Committee Standard, 2024 Edition (Washington, DC: U.S. Department of Homeland Security, 2024)



Review of foundational literature.

4 Steps to Putting ESRM Into Practice

In 2019, ASIS International, a leading membership organization for security professionals and global source of security standards, published the Enterprise Security Risk Management (ESRM) Guideline. In the years since, ESRM has become a well-known and widely practiced discipline in corporate security focused on aligning organizational strategy, resources, and risk. Perhaps most importantly, ESRM helps corporations think holistically about security, looking across a wide range of security functions in a unified manner. The ESRM cycle, detailed in the Guideline, includes four steps:

1. **Identify and Prioritize Assets:** Who is responsible for which assets, and how valuable are those assets to the company?

2. **Identify and Prioritize Risks:** What risks are posed to certain assets, and which of those risks are most salient?

3. **Mitigate Prioritized Risks:** Which risk treatment strategy (i.e. transfer, spread, avoid, mitigate) should be implemented for a particular risk-asset pair?

4. **Continuous Improvement:** What can be learned from security incidents, and how can that information be shared and implemented effectively?



Source: © 2019 ASIS International. Source-ASIS International, Enterprise Security Risk Management Guideline. Used with permission.

While the ESRM Guideline lacks the depth and specificity of the ISC Standard, it was written specifically with the private sector in mind. ESRM places security risks, including political risks, in a broader business context and is a useful tool for security professionals who want to link security risks and threats to business impact.

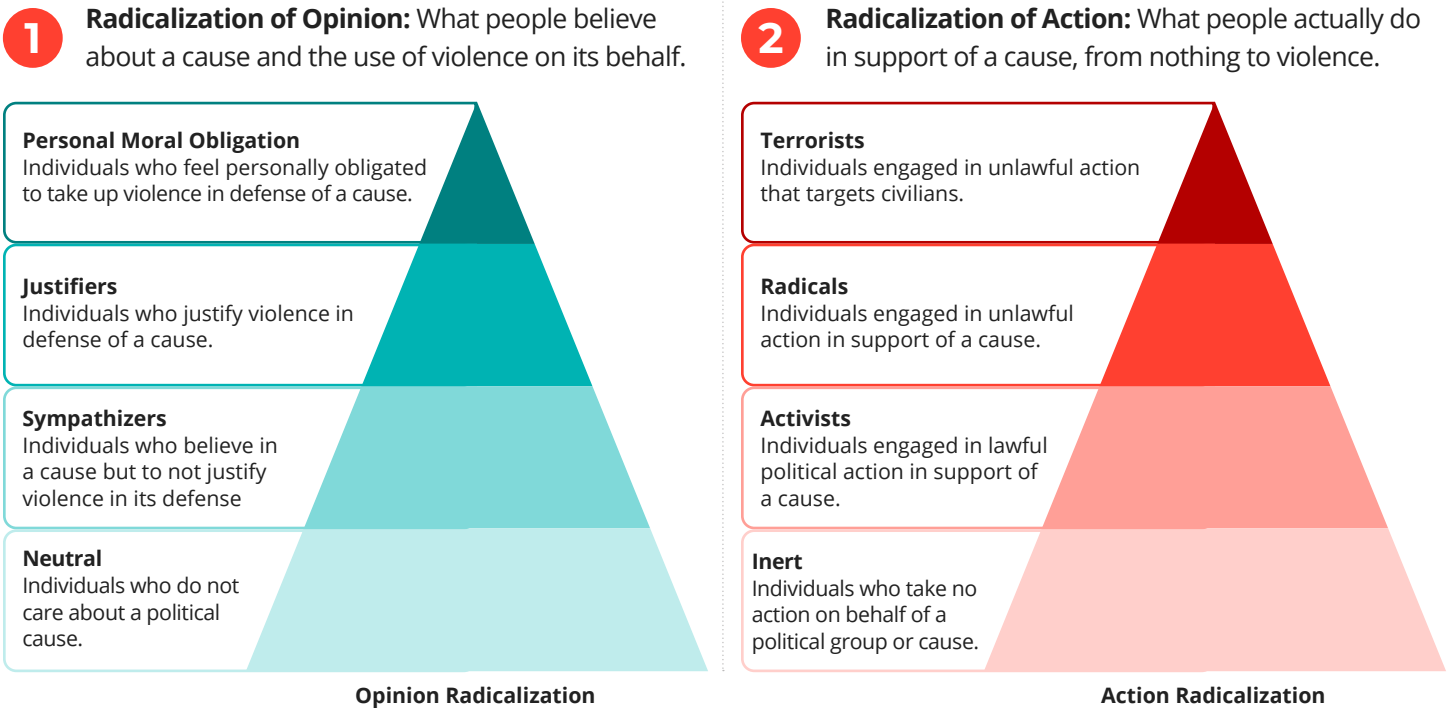
ASIS Enterprise Security Risk Management Guideline: Access Here

Review of foundational literature.

The Two-Pyramids Model

The Two-Pyramids Model is an academic framework focused on understanding political radicalization and identifying the precursors of terrorist violence. The model distinguishes between two related but separate processes: the radicalization of opinion and the radicalization of action. The core insight is that holding extreme views and committing extreme acts do not always go hand in hand, and that understanding the gap between the two is key to assessing potential threats.

The model was developed in 2017 by Clark McCauley, Research Professor of Psychology and co-director of the Solomon Asch Center for Study of Ethnopolitical Conflict at Bryn Mawr College, and Sophia Moskalenko, a social psychologist then in the Department of Psychology at Bryn Mawr College, whose work focuses on radicalization, terrorism, and political violence. The research was supported by DHS through the National Consortium for the Study of Terrorism and Responses to Terrorism (START), a leading academic center for the study of terrorism at the University of Maryland (UMD).



Graphic derived from: Clark McCauley and Sophia Moskalenko, "Understanding Political Radicalization: The Two-Pyramids Model," American Psychologist 72, no. 3 (2017): 205–216.

The model was developed primarily to help U.S. security officials understand the radicalization process among jihadist networks. It has been used to map how individuals and groups move from grievance to action, and to identify intervention points along that path.

The model's value for corporate security practitioners lies in its practical structure. By distinguishing opinion radicalization from action radicalization, it gives security teams a way to taxonomize political violence and instability risk, moving beyond broad threat categories toward a more granular picture of who poses a genuine threat to the organization, and in what way. This level of analytical precision supports more proportionate, effective responses, and reduces the risk of either overreacting to political expression or underreacting to genuine behavioral warning signs.

The Two-Pyramids Model: Access Here

SECTION 04

Threat environment: Political violence & instability in the US.

At the time of writing in late summer 2026, just weeks prior to the 2026 midterm elections, the political environment facing corporations in the United States is complex and multifaceted. To gain a granular understanding of the different ways in which political violence and instability risks may manifest, this analysis examines risks across three tiers of descending severity:

TIER 1 Political violence with intent to harm, including terrorism

TIER 2 Unlawful civil disobedience, property destruction, and similar activity

TIER 3 Lawful activism and demonstration

For each of these categories, we discuss risks related to political actions and those related to political expressions.

Political actions vs. expressions.

Political Actions

Political actions include demonstrations, boycotts, walkouts, strikes, sit-ins, blockades, shareholder activism, coordinated campaigns, civil disobedience, direct action, terrorism, and any other organized conduct undertaken to advance or oppose a political, social, or policy objective.

Political Expressions

Political expressions include statements, social media posts, op-eds, interviews, sponsorships, endorsements, and the display of symbols, signage, or messaging that communicate a position on a political, social, or policy issue.

Expressions and actions are not always independent.

Expression is sometimes deployed deliberately to provoke or organize action. In some cases, this is called incitement. However, in other cases, the purpose of the expression can be harder to ascertain.

One recent example of how blurry the line between expression and action can be is the proliferation of "Wanted" posters bearing the names and photos of corporate executives across U.S. cities in the wake of Brian Thompson's murder. None of these executives were killed after the posters went up, but had they been, would the posters' creators be responsible for inciting murder?

There have been examples of online conspiracy theories driving lone actors to violence. On December 4, 2016, Edgar Maddison Welch fired a rifle inside Comet Ping Pong, a Washington, D.C. pizzeria, after traveling from North Carolina to "self-investigate" the fabricated "Pizzagate" conspiracy theory, a stark illustration of an online narrative culminating in an armed attack despite never directing anyone to commit violence.

Finally, sophisticated threat actors, including foreign nation states, may purposely stay below the threshold of action or incitement, leveraging mis- and dis-information to create real-world effects. Russian state-linked influence operations, for example, have a documented history of amplifying both sides of divisive domestic disputes with the apparent aim of deepening polarization and provoking unrest rather than advancing any single cause.

The Definition of Incitement

According to Cornell Law School, to "incite" means to "instigate or to persuade another to commit a crime." 18 U.S. Code § 2102 states that inciting a riot involves "urging or instigating other persons to riot," but notably that it does not involve "the mere oral or written advocacy of ideas or expression of belief" that do not advocate for violent acts.

TIER 1

Political violence with intent to harm, including terrorism.

Political Actions

The threat from both domestic and foreign extremism in America will remain high for the foreseeable future, according to DHS's 2025 Homeland Threat Assessment, published in October 2024 and the most recent such assessment from the agency. This assessment is supported by the statistics. From 2023-2025, there were nearly 3,000 incidents of terrorism and targeted violence across the nation, with a 30% increase in incidents between 2024 and 2025. Roughly a quarter of those incidents produced casualties, resulting in 491 victim deaths and 1,231 victim injuries.

~3,000
incidents of terrorism and targeted violence, 2023–2025

+30%
increase in incidents between 2024 and 2025

491
victim deaths from incidents producing casualties

1,231
victim injuries across the same period

Source: START Terrorism and Targeted Violence in the United States (T2V) Database

Incidents specifically targeting corporate executives reached their highest level on record in 2025, doubling the 2024 total worldwide, with activism the single largest category of recorded motivations. In June 2026, the U.S. Secret Service and Federal Bureau of Investigation (FBI) thwarted a terror plot allegedly intended to kill attendees of the UFC event hosted on the White House lawn. According to the charging documents, the group identified a target list that included government officials and business executives, and was driven by anti-government accelerationist beliefs, conspiracy theories, and hostility toward corporate greed (among other political grievances).

Executive targeting incidents in 2025 doubled the 2024 total worldwide, the highest level on record.

Activism was the single largest category of recorded motivations behind executive-targeting incidents in 2025.

Source: Security Executive Council

TIER 1

Political violence with intent to harm, including terrorism.

Political Expressions

Rhetorical support for terrorism and political violence is generally protected by the First Amendment and not a crime, absent a specific, credible threat, incitement to imminent violence, or close coordination with a foreign terrorist organization. The public response to Brian Thompson's killing illustrated this. Many celebrated the killing online and lionized the killer.

280%

month-over-month increase in incidents targeting local public officials in September 2025, the highest monthly total of the year.

~75%

of local officials reported being less willing to engage in at least one key political activity due to concerns about hostility, by Q3 2025.

Source: Bridging Divides Initiative

Other high-profile murders have evoked similar surges in rhetorical support for political violence as well as targeted threats. Following Charlie Kirk's assassination in September 2025, the Bridging Divides Initiative recorded a 280% month-over-month increase in incidents targeting local public officials in September, the highest monthly total of the year, and by the third quarter of 2025, nearly 75% of local officials reported being less willing to engage in at least one key political activity due to concerns about hostility.

It should be assumed that high-profile acts of political violence may now consistently produce cascading rhetorical escalation, and that escalation carries its own operational risks for corporate security teams.

> **The mere advocacy of political or social positions, political activism, use of strong rhetoric… does not constitute violent extremism and is constitutionally protected.**
>
> — Federal Bureau of Investigation & U.S. Department of Homeland Security, Strategic Intelligence Assessment and Data on Domestic Terrorism, 2023

TIER 2

Unlawful civil disobedience, property destruction, & similar activity.

Political Actions

Civil disobedience, property destruction, and other unlawful activity present a direct risk to corporate operations. These risks can manifest either as unlawful activity directed at a specific company or brand, or as spillover from activity targeting other companies or broader unrest.

An example of property destruction intended for a specific brand is the 2025 wave of Tesla attacks across the United States. This series of deliberate, ideologically motivated incidents targeting dealerships and vehicles was inspired by Elon Musk's strong public association with the Trump administration. While these attacks seemingly did not intend to kill, they were illegal and resulted in significant property and financial losses.

But companies can also be impacted when politics has nothing to do with them. During 2020 protests sparked by the murder of George Floyd, at least a dozen bank branches, including some belonging to Wells Fargo, were damaged or lost entirely.

Recommended guidance from CISA:

Establish direct communication with local law enforcement and fusion centers ahead of planned demonstrations. Use these relationships to understand when events may escalate into unlawful activity, identify potential threats to nearby businesses and residents, and prepare appropriate security measures in advance.

Source: Cybersecurity and Infrastructure Security Agency Protecting Infrastructure During Public Demonstrations, 2025

Political Expressions

Rhetorical support for direct action, civil disobedience, and property destruction is a meaningful early warning signal, even when it stops short of incitement. Online calls to action and the public identification of corporate facilities or executives can precede and directly enable unlawful activity.

The Tesla attacks, for example, were preceded by sustained online rhetoric casting the company as a political target, a pattern that, in hindsight, provided advance indicators of escalation.

In a November 2025 survey by the Brookings Institution, over 20% of respondents expressed support for political violence, a level consistent with recent years, demonstrating a sustained level of heightened rhetorical support for unlawful political activity.

20%+

of respondents expressed support for political violence in November 2025, a level consistent with recent years.

Source: Brookings Institution (2025)

TIER 3

Lawful activism & demonstration.

Political Actions

Lawful activism and demonstration have surged in recent years. The non-profit organization Armed Conflict Location & Event Data (ACLED) recorded nearly 20,000 demonstrations in the United States in 2025, marking a 77% increase from 2024 and the highest yearly total since 2020. Peaceful activism and demonstrations are constitutionally protected and do not pose an inherent threat. The data bears this out: violent or contentious activity was reported at just 0.5% of demonstrations in 2025, meaning the vast majority of participants exercised their rights lawfully and without incident.

Demonstrations recorded in the United States
By year, with share of demonstrations reporting violent or contentious activity in 2025



+77%
year over year

0.5%
reported violent or contentious activity

Source: Armed Conflict Location & Event Data (ACLED), 2025.

However, demonstrations of sufficient scale can disrupt local logistics, restrict access to facilities, and affect day-to-day operations. A sustained 2026 activist campaign against Citizens Bank illustrates this: despite having no operational role in immigration detention, the bank's financial affiliation with two U.S. Immigration and Customs Enforcement (ICE) contractors made it a recurring target of coordinated branch protests, a shareholder-meeting demonstration, and account withdrawals, including a 7-figure sum pulled by one organization alone, with further withdrawals threatened.

> **First Amendment demonstrations are a fundamental right in the United States. However, they also have significant potential to impact business operations.**
>
> — Maryland Department of Emergency Management, Business Resource Guide for First Amendment Demonstrations

TIER 3

Lawful activism & demonstration.

Political Expressions

Rhetorical support for lawful protest, such as sharing event information, encouraging attendance, or publicly endorsing a cause on social media, is the expressive counterpart to physical participation. It is commonplace, constitutionally protected, and poses no inherent threat on its own. A 2026 analysis of online activism discourse found violent or confrontational language in just 6% of posts, according to Liferaft's threat data, most of it rhetorical comparison to past unrest rather than advocacy for new violence.

That said, this kind of expression is worth tracking for three main reasons.

1. **A significant uptick in online organizing or activist rhetoric around a particular issue or location can serve as an early signal that physical demonstrations, and any associated disruption, are likely to follow.**
2. **Expressions of support by employees on social media and other public platforms can create reputational exposure for the organization, independent of any security risk.**
3. **Certain expressions of support may serve as an early indicator of an individual's radicalization. This category requires particular care: the line between protected political expression and a genuine warning sign is narrow, easily misjudged, and carries serious consequences if drawn incorrectly.**

LIFERAFT DATA

4,223

online posts about America 250 events over a seven-week span

22%

of those posts included counter-mobilization language

June 2026 data from Liferaft revealed online posts about America 250 events over a seven-week span leading up to the celebration.

> **It is most important to look critically and contextually at the specific actions of individuals and their intent.**
>
> — FBI, US Violent Extremist Mobilization Indicators, 2025

Ideologies & motivations.

Political violence in the United States is driven by a range of ideologies and motivations. While the threat from each changes with time, and increasingly there are some individuals who have a mishmash of ideologies (what former FBI Director Chris Wray called "salad bar ideology"), some general categories of threat actor have remained consistent for decades. One widely used framework for taxonomizing these ideologies, START's Profiles of Individual Radicalization in the United States (PIRUS), buckets radicalized individuals into four categories.

1

Far-Right Extremism

Far-right extremism spans white supremacist, anti-government, and militia movements, and has historically been the largest source of domestic terrorism activity in the United States. Named groups associated with this category include Atomwaffen Division and various militia and "boogaloo" networks. Recent attacks include the 2022 Buffalo supermarket shooting and the 2019 El Paso Walmart shooting.

2

Far-Left Extremism

Far-left extremism includes anarchist, anti-fascist, and revolutionary socialist movements, generally oriented around anti-capitalist or anti-authoritarian grievances. This category encompasses loosely organized anarchist and anti-fascist networks operating under the Antifa banner, along with smaller revolutionary socialist groups. Recent activity includes property destruction during 2020's period of civil unrest and a 2025 armed attack on an ICE facility in Alvarado, Texas.

3

Islamist Extremism

Islamist extremism encompasses jihadist violence, whether directed by a foreign terrorist organization or carried out by an individual who radicalized independently. Al-Qaeda and ISIS remain the most significant global jihadist organizations. Recent attacks include the 2016 Pulse nightclub shooting and the January 2025 vehicle attack on Bourbon Street in New Orleans, both carried out by individuals who pledged allegiance to ISIS.

4

Single-Issue Extremism

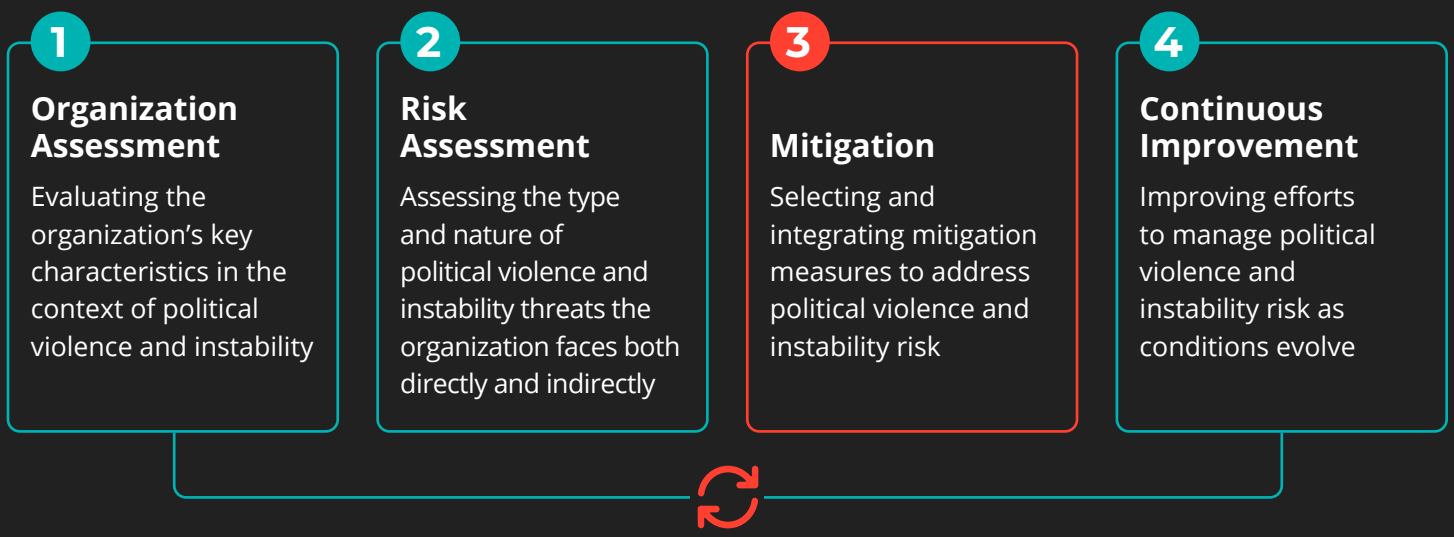
Single-issue extremism captures actors organized around one narrow cause rather than a broader ideological worldview. Historical and ongoing examples include anti-abortion violence, such as the 2015 shooting at a Colorado Springs Planned Parenthood clinic; animal rights and environmental extremism; and, in earlier decades, Puerto Rican nationalist groups such as the Armed Forces of National Liberation (FALN).

In addition to START, the FBI and the National Counterterrorism Center (NCTC) maintain their own taxonomies for domestic and international terrorism, respectively. FBI's domestic categories include: racially or ethnically motivated violent extremism, anti-government/ authority violent extremism, animal rights/environmental violent extremism, and abortion-related violent extremism. NCTC focuses on foreign terrorist organizations and the homegrown violent extremists they inspire, including Islamist extremist/jihadist groups, Iran-linked extremist groups, revolutionary and separatist groups, and cartels and gangs.

SECTION 05

A framework for managing the risk of political violence & instability to corporations.

This framework is intended for corporate security and intelligence teams seeking to manage the risk of political violence and instability to their organizations. The framework, based on similar concepts like the ISC's Risk Management Process Standard and the ASIS ESRM Guideline, includes four phases that form a closed loop:



Each phase includes:

- **Overview:** a summary of that phase of the cycle and its importance;
- **Key Elements:** the major considerations corporate security and intelligence teams should be aware of when implementing this phase; and
- **Checklist:** a quick reference guide for practitioners to use in real-time.

PHASE 1 OF 4

Organization assessment.

Overview

Organization assessment determines whether, why, and to whom an organization is an attractive target for political violence or other political actions. From the perspective of terrorists, extremists, and others who use or support violence to achieve political objectives, target selection is fundamental. Therefore, corporate security and intelligence practitioners must look at their own organization through this lens, imagining how it could be perceived by a wide range of actors who may adopt political violence. Assessing the organization is a critical first step in managing the risk of political violence and instability because it provides vital context for understanding particular threats and potential mitigations.

Key Elements

The organization assessment should consider at a minimum the following five factors:

Industry

Targeting of a particular organization for political violence often starts with its industry classification. For example, certain groups, actors, or movements have negative views of the energy sector, financial services sector, data center sector, or others based on those actors' ideologies and objectives. Moreover, if your organization does business with a targeted sector, you may be targeted based on that association (e.g., a bank that is targeted by an environmentalist extremist organization because it financed a fossil fuel project). This is a form of what we term associative risk: exposure an organization inherits not from its own conduct but from its business relationships, clients, vendors, and industry affiliations.

Geography

An organization's geography (i.e., the location of its facilities and other assets) plays a significant role in its exposure to potential political violence or instability. Within the United States, some regions and states are more prone to certain types of political violence, and cities are more likely to attract large demonstrations than rural areas. Corporate security teams should map the organization's full geographic footprint and taxonomize locations and assets by function, so that each site can be assessed for its local political climate, proximity to prior incident clusters, and the vicinity of local law enforcement capacity, among other factors.

Symbolic value

In the 9/11 attacks, al-Qaeda targeted symbols: the World Trade Center because it represented American financial might and the Pentagon, America's military might. The fourth plane was intended for the Capitol or White House: political might. Symbols are critically important in political violence. Organization assessment must examine the company's symbolism, both how it is perceived in the mainstream and by fringe groups and conspiracy theorists. Brand associations with contested issues, iconic or recognizable physical assets, cultural prominence, and any role as a stand-in for a broader grievance can all elevate an organization's symbolic value, and this can drive bad actors' target selection. Companies in multi-tenant buildings warrant particular attention here, since a company can inherit symbolic exposure simply by sharing a building with another tenant that is a potential target.

PHASE 1 OF 4

Organization assessment.

Scale

Organizational scale changes a company's exposure to political violence and instability. Large enterprises attract disproportionate attention but command more resources to defend themselves, while smaller organizations may be less likely to draw national attention but are softer targets. Controversial actions by industry leaders can create risk for smaller companies in the same sector, who may lack the security resources to defend themselves.

Notable executives

The public profile of an organization's executives can expose the company to risk, regardless of the organization's own industry or symbolic value. High-visibility executives, Political Action Committee (PAC) activity, lobbying positions, and board or client relationships all have the potential to increase political violence and instability risk.

Organization Assessment Checklist

- Determine your organization's industry classification as well as those of major publicly known customers and suppliers, and evaluate political sensitivity
- Consider the symbolic nature of your organization, its products and services, and your industry
- Classify geographic footprint and company size, and evaluate resulting exposure
- Assess the public profiles of notable executives for political positions that may create additional risk to the company
- Produce a written report and set a review trigger for material changes

While there is no one-size-fits-all template for an organization assessment, a good starting point is a short written report that covers the above factors and is reviewed for updates at least annually, or when major developments occur.

73%

of lone-offender terrorists studied by the FBI selected targets because they were instrumental to their goal or ideology.

47%

of those offenders also selected targets based on symbolic value.

Source: FBI Behavioral Analysis Unit, A Study of Lone Offender Terrorism in the United States (1972–2015), 2019.

PHASE 2 OF 4

Risk assessment.

Overview

Whereas the organization assessment focuses internally, the risk assessment focuses externally. It is intended to characterize the type and nature of political violence and instability risks an organization faces both directly and indirectly. The risk assessment is critical in helping the security intelligence team calibrate effective responses to a wide range of political expressions and actions, thereby "threading the needle" between overreaction and underreaction.

As with all security risk assessments, one focused on political violence and instability should examine the threats, vulnerabilities, and consequences related to these issues and link them to the assets identified during the organization assessment phase. It should also estimate the likelihood and impact of these risks, either qualitatively or quantitatively. It is important to note that the methodology and rigor for a security risk assessment is highly unique to the organization. When assessing political violence and instability, corporate security teams should not create a separate siloed process; instead, they should integrate these considerations and assessments with existing workflows.

Key Elements

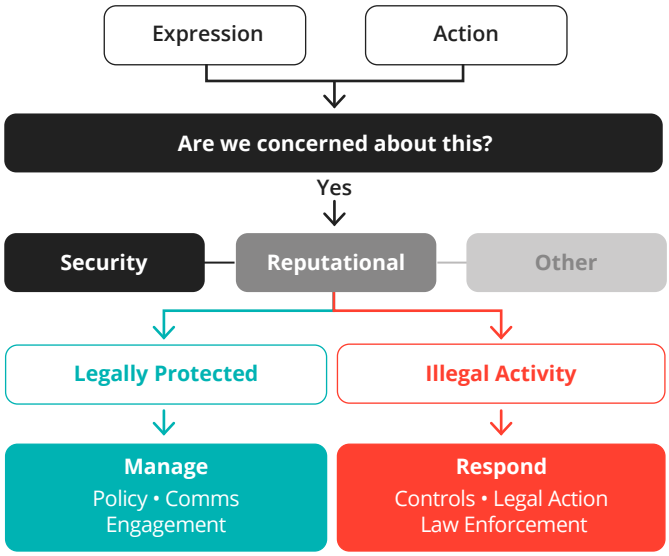
Given the complexity of the U.S. political environment and the sometimes-blurred lines between political expression, action, and violence, a key objective for any risk assessment on political violence and instability should be to provide clarity from obscurity, ultimately informing decision-making that is carefully calibrated to the type and nature of the risk.

Specifically, the assessment should help the corporate security team understand which political expressions and actions may pose a risk to the organization, and which do not. Of those that do pose a risk, the assessment should uncover whether that risk is a security issue, a reputational issue, or something else. And finally, some risks will be found to stem from legally protected expression and action while others are the result of illegal activity. This must also be examined during the assessment to inform appropriate mitigation.

Assessing Political Expressions & Actions

Both political expressions and actions may pose a risk to the organization. When identifying a new expression or action, such as a social media post associating the company with a political issue (expression) or a planned demonstration near the company's offices (action), the corporate security team should ask whether that action or expression is a potential cause for concern to the organization. To evaluate whether the expression or action is concerning, the security team should consider which tier (lawful activism, unlawful disobedience, terrorism, etc.) seems to be most relevant. If there is clearly no cause for concern, no further action is required. Otherwise, the team should progress to considering what type of risk the expression or action might pose.

Triage Logic for Corporate Security Teams



PHASE 2 OF 4

Risk assessment.

Distinguishing between security risks, reputational risks, and other risks

A security risk threatens the physical safety of people or the continuity of operations, facilities, and assets, such as a demonstration that could lead to physical confrontations outside an office, or a targeted threat against an executive. A reputational risk threatens the organization's brand, stakeholder trust, or market position through association or perception, such as a widely shared post framing the company as complicit in a contested political issue. Other risks may be principally regulatory, financial, or operational in nature and warrant their own treatment. Importantly, expressions may pose a security risk (e.g., incitement) and actions may pose reputational risk (e.g., lawful and peaceful demonstration).

Assessing legality

Some expressions and actions that pose risk to the organization are nonetheless lawful, exercising constitutionally protected rights to speech, assembly, and petition; others cross into illegal activity. This distinction is fundamental because it governs the response available to the organization.

Legally protected conduct, e.g., a permitted protest outside company offices, or a critical but truthful public statement, should typically be addressed through means such as policy, communications, and engagement. Illegal conduct, e.g., trespass, vandalism, harassment, or a credible threat against personnel opens different options, including protective measures, legal action, and referral to law enforcement. It is essential that corporate security teams consult with legal counsel in assessing the legality of political expressions and actions, as well as the legality of different mitigation options. Legal counsel is a key partner in ensuring the risk is assessed correctly and responses are proportional, avoiding over- or underreaction.

Intelligence and information sharing

Risk assessment depends on current intelligence. Corporate security and intelligence teams should work closely with Information Sharing and Analysis Centers (ISACs), state and regional fusion centers, and federal, state, and local law enforcement to ensure situational awareness, particularly during periods of heightened unrest. These channels are a critical complement to internal open-source intelligence (OSINT) tools and platforms.

Risk Assessment Checklist

- Adapt the triage process included above to your organization and existing risk assessment methodologies
- Engage early with legal counsel to ensure the corporate security team understands the difference between legal and illegal expressions and actions, as well as corresponding mitigation options
- Taxonomize the types of risks most important to your organization: security, reputation, etc.
- Identify data sources (both tools and partners) best suited for providing intelligence and threat data that can inform the risk assessment process

PHASE 3 OF 4

Mitigation.

Overview

Following the completion of an organization assessment and risk assessment, the corporate security team can move to mitigation. This involves the selection and implementation of security controls that reduce the likelihood or impact of risks identified. It is of particular importance in the context of political violence and instability that mitigation measures be calibrated to the nature, type, and severity of the risk posed. Over-zealous mitigation of legally protected political speech, for example, is likely to cause more harm to the organization than the speech itself.

Likewise, as with the risk assessment process, political violence and instability risk mitigation should be integrated across the existing corporate security and intelligence program rather than built as a separate stovepipe.

Key Elements

Effective mitigation of political violence and instability risks requires weaving these considerations into the various functions of the corporate security and intelligence program, including the following:



Intelligence

Intelligence is the function that converts a static risk assessment into ongoing warning, giving the corporate security team the lead time to act before a political expression or action escalates toward violence. Intelligence teams should treat political violence and instability as standing collection requirements rather than ad hoc queries during periods of volatility: tasking analysts against the specific actors, grievances, and locations surfaced in the risk assessment, and building the relevant liaison relationships. State and regional fusion centers are an underused source of real-time situational intelligence during civil unrest, and contract security personnel with local ties frequently surface neighborhood-level indicators that national monitoring tools miss.

Organizations should have an OSINT program spanning surface and dark web, social media, and relevant online forums, as well as collection processes reviewed regularly with legal counsel to keep monitoring inside legal and reputational bounds.



Physical security

Physical security is most directly responsible for protecting people, facilities, and operations when a political action materializes as a demonstration, blockade, or attack against a specific site. Physical security posture should flex with the real-time threat picture, so that protection scales to the criticality and symbolism of each facility rather than applying a uniform standard across the portfolio. The ISC's five-factor Facility Security Level methodology — mission criticality, symbolism, population, size, and threat — provides a defensible basis for that calibration.

Organizations should develop layered protection matched to facility level; pre-staged protective materials that can be deployed on short notice; and a scalable up-and-down protocol, such as boarding up retail facilities overnight when local conditions warrant and reopening by day once the risk has passed.

PHASE 3 OF 4

Mitigation.

Cybersecurity

Political grievances can manifest as cyber threats. A company that becomes associated with a contested political issue is a natural target for hacktivism, for example. The characteristic hacktivist methods, such as distributed denial-of-service (DDoS) attacks, website defacement, doxxing, phishing and spear-phishing campaigns directed at employees, and the theft and leaking of sensitive data to inflict reputational harm, should be treated as foreseeable consequences of political exposure.

Mitigations include DDoS protection and web-application defenses sized to withstand disruption during periods of heightened political attention; monitoring for credential leaks, defacement, and data dumps characteristic of hacktivist campaigns; standard, recurring employee training on identifying phishing and spear-phishing attempts, reinforced during periods of heightened political risk; and an incident-response plan that connects the cyber team to intelligence, communications, and legal.

~10%

of all claimed **hacktivist** DDoS attacks worldwide in 2025 targeted the United States, making it the second-most targeted country globally.

Outside the US, the trend is equally pronounced. Across the EU, nearly 80% of incidents analyzed by ENISA were attributed to hacktivism, with ideological motives driving almost 80% of assessed incidents.

Sources: ENISA, ENISA Threat Landscape 2025; Radware, 2026 Global Threat Analysis Report

Executive protection

Corporate executives are the human faces of a company. As a result, they face particular risk when the company has become associated with a contested issue. Executive protection programs, which include corresponding intelligence, threat management, and protective measures, should be calibrated to account for the political environment.

In a heightened political violence threat environment, the executive protection team may choose to increase protective intelligence efforts focused on threats to named principals; residential and travel security; and digital footprint reduction, with home address and family exposure warranting particular attention, since these are often the softest vulnerabilities.

Insider threat and workplace violence

Employees can pose a direct threat to the companies they work for or may facilitate access for an outsider targeting the organization for political reasons. Insider threat teams should review risk indicators regularly to ensure they account for evolving political and ideological issues that may drive an insider to act against the organization. Because insider threat countermeasures touch upon employment and privacy, they should be built and run in coordination with human resources (HR) and legal counsel.

Meanwhile, a contested political environment can increase the risk of violence in the workplace, either among employees or from an outsider (e.g., an active shooter). Workplace violence prevention programs should account for politically or ideologically motivated behavior, and build multidisciplinary capability (e.g., across security, HR, legal, and mental health) to assess and manage a person of concern rather than simply removing them and hoping the risk leaves with them.

PHASE 3 OF 4

Mitigation.

Reputation management

Political issues may impact a company's reputation in numerous ways, from the positions it takes or declines to take, to the customers, partners, and causes it is associated with, to the way it responds when a political controversy reaches its doorstep. Managing that exposure is principally the work of the communications, public relations, and corporate affairs functions, which weigh brand, stakeholder trust, and market position. The corporate security team's role is to remain aware of this reputational dimension and to ensure its protective decisions do not undercut it, since a heavy-handed security posture toward lawful political activity may itself become a reputational event.

Security and communications should therefore develop a shared understanding of roles before an incident occurs. This collaboration can be sharpened through jointly owned crisis response and de-escalation playbooks, a clear separation between protective and incident coordination roles, and pre-established lines of communication that keep security, communications, and legal aligned in real time.

Crisis management and business continuity

This function is what keeps the organization operating when a political violence event moves from threat to disruption. It is distinct from physical security, which protects the asset, and from reputation management, which handles external perception; continuity is concerned with the resilience of the business itself once an incident is underway.

Political violence and similar crises should be named scenarios within existing continuity and crisis management plans. Also important are pre-established decision thresholds for facility closure, evacuation, and relocation as well as tested activation and communication protocols that reach affected employees in real time.

> **The scope of security countermeasures is commensurate with the risk posed to the facility.**
>
> — Interagency Security Committee, The Risk Management Process, 2024

Mitigation Checklist

- Evaluate the extent to which political violence considerations are woven into existing corporate security and intelligence functions
- Where appropriate, build new plans, policies, and procedures focused on political violence and instability but nested within these standing functions
- Ensure close and early coordination with other organizational stakeholders, especially legal, HR, and communications
- Stand up a security-communications playbook, and consider a dedicated incident management function
- Test decision thresholds and activation protocols through regular tabletop exercises

PHASE 4 OF 4

Continuous improvement.

Overview

Risks related to political violence and instability are dynamic. The actors, grievances, and tactics an organization faces evolve with shifts in the political environment, and the organization itself changes as it adds new facilities, new executives, new business relationships, and new public positions. Continuous improvement is the phase that keeps the framework current amid these shifts. In practice, it means treating the prior three phases as living products: organization assessment, risk assessment, and mitigation are revisited on a set cadence and in response to triggering events, with the output of each review feeding back into the next cycle. A program that is assessed once and left in place will steadily drift out of alignment with the threat it was built to address.

Key Elements

Effective continuous improvement rests on a handful of practices, each nested within the standing corporate security and intelligence program rather than run as a separate exercise.

Review cadence and triggers

A scheduled review of organization assessment, risk assessment, and mitigation at least annually establishes the baseline, supplemented by event-driven reviews when material developments occur. Defining these triggers in advance keeps the program responsive without waiting for the next scheduled cycle.

Measurement

Improvement should be assessed rather than assumed. Track metrics over time, such as intelligence warning lead time, speed of protective posture changes, incident and near-miss frequency, and the currency of key assessments give teams a defensible basis for judging whether mitigations are working and where to direct further effort.

Learning from events

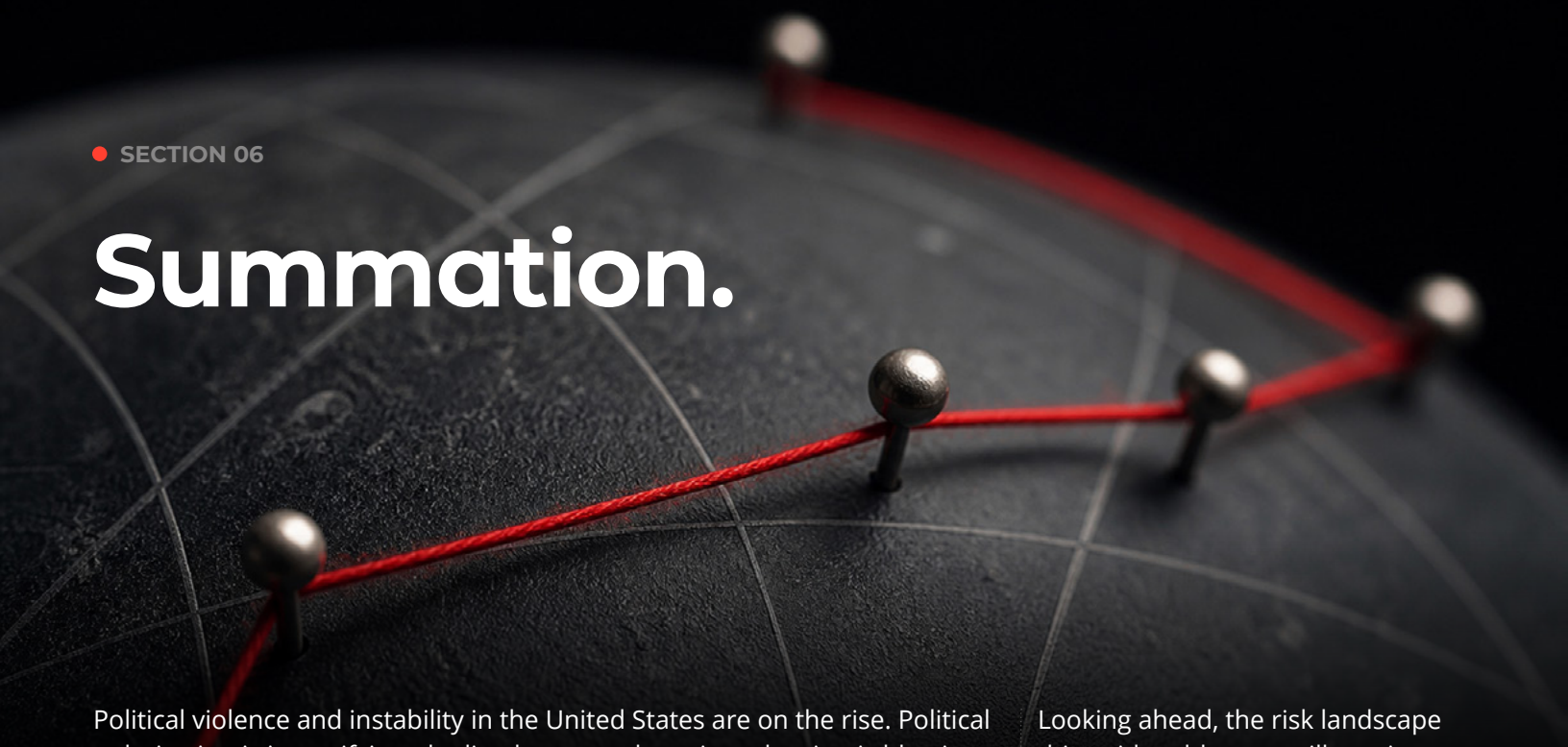
Incidents are the most direct evidence of where an assessment or mitigation fell short, and each should be examined for what it reveals. After-action reviews of incidents and near misses should feed structured lessons back into the program, and incidents affecting comparable organizations should be monitored for transferable insight, allowing the organization to learn without having been the target.

Feedback and ownership

The value of a review lies in what happens to its findings. Results should be routed back to the owners of the relevant security function and, where they change the organization's risk picture, back into the organization and risk assessments themselves. Because continuous improvement touches every function, it works best when ownership is explicitly assigned to a named team or individual.

Continuous Improvement Checklist

- Set a review cadence for each phase (at least annual) and define the event-driven triggers that prompt an off-cycle review
- Conduct after-action reviews of internal incidents and near misses, and monitor incidents affecting peer organizations for transferable lessons
- Track a small set of program indicators over time to gauge whether mitigations are working
- Route review findings back to security function owners and, where warranted, back into the organization and risk assessments
- Assign clear ownership for the continuous improvement process



SECTION 06

Summation.

Political violence and instability in the United States are on the rise. Political polarization is intensifying; the line between rhetoric and action is blurring, and businesses and their executives are increasingly targeted for what they are perceived to represent. In this environment, corporations must prioritize political violence and instability as key risks and establish a framework for proactive assessment and mitigation.

Effective management of political violence and instability risk depends on a disciplined, repeatable process. To date, there has been very little in the literature specifically designed for helping corporations build such a process. In this guide, we introduced a new framework for managing political violence and instability risks to corporations, based on well-established government, industry, and academic literature and best practices.

This four-phase framework provides a structured method that corporate security and intelligence teams can use to evaluate their organization's key characteristics in the context of political violence and instability; assess the type and nature of related threats the organization faces both directly and indirectly; select and integrate mitigation measures to address risks related to political violence and instability; and improve efforts to manage political violence and instability risk as conditions evolve. As emphasized throughout this guide, distinguishing which political expressions and actions actually pose a risk to an organization, and whether that risk is a security matter, a reputational one, or both, is foundational to this process.

This guide is intended as a practical resource that practitioners can use regardless of program maturity. The checklists and examples are intended to help a wide range of corporate security practitioners across industries and levels of seniority bring greater discipline and rigor to their efforts to address political violence and instability risks to their organization.

Looking ahead, the risk landscape this guide addresses will continue to evolve. This report should therefore be viewed as a living reference. As organizations enhance their political violence and instability risk management efforts, the principles outlined here can be adapted to reflect emerging risks, new tools, and lessons learned.

Ultimately, managing political violence and instability risks is a governance and enterprise risk issue. It requires close, early coordination between security, legal, HR, communications, and other stakeholders. Further, it should be expected that in many cases political violence and instability issues will draw the interest and attention of the Board and C-suite. When political violence and instability considerations are integrated effectively into an organization's broader risk management program, that organization is better positioned to protect its people, its operations, and its reputation.

SECTION 07

Resources you can use.

Standards, Guidelines, and Academic Literature

ASIS ESRM Guideline
Aligns corporate security strategy with business risk management

ASIS Security Risk Assessment Standard
Guidance for conducting a security risk assessment

ISC Risk Management Process Standard
Five-step methodology for securing federal government facilities

Understanding Political Radicalization
The Two-Pyramids Model — Academic framework explaining radicalization from opinion to action

TRAP-18
Assessment protocol for mitigating the threat of targeted violence

Liferaft Report
Threat Brief: Heightened Vigilance Through America250, 2026

Terrorism Databases & Taxonomies

START Terrorism and Targeted Violence in the United States (T2V) Database
A comprehensive record of terrorism and targeted violence in the United States

START Global Terrorism Database (GTD)
Open-source database including information on terrorist events around the world from 1970 through 2020

START Profiles of Individual Radicalization in the United States (PIRUS)
Academic taxonomy of domestic terrorist movements and ideologies with an accompanying dataset

ACLED Incident Tracker
Real-time database tracking terrorism incidents in the United States and Canada

NCTC Counterterrorism Guide
Intelligence community taxonomy of global terrorist movements and organizations

FBI Domestic Terrorism: Definitions, Terminology, and Methodology
Federal law enforcement taxonomy of domestic terrorist movements and ideologies

SECTION 08

About the authors.



Mark Freedman

Mark Freedman is Principal and CEO of Rebel Global Security (RGS), a Washington-based firm that provides national security advice to the private sector. RGS helps businesses navigate global and national security dynamics to achieve commercial success.

For almost a decade, Mark served as a U.S. State Department officer, including as Chief of Staff to the Ambassador-at-Large for Counterterrorism. As Chief of Staff, Mark played a key role in the State Department's global counterterrorism strategy, policy, and planning during the height of the threat from ISIS in the mid-to-late 2010's.

In previous assignments at State, Mark led interagency surge teams to tighten security cooperation with European allies in the wake of the 2015 ISIS attacks in Paris; developed strategic plans to contain weapons proliferation to terrorists during the Arab Spring; and created a first-of-its-kind multilateral forum for counterterrorism information sharing.

Mark holds a M.A. in Security Studies with a concentration in Terrorism and Counterterrorism from Georgetown University and a B.A. in International Affairs from The George Washington University. He is a Certified Protection Professional (CPP).



Rachel Kronenfeld

Rachel Kronenfeld is a Licensed Investigator and Suite Product Manager at Liferaft.

Rachel's career has seen her don multiple hats and emerge as a trailblazer in the realm of OSINT and investigations. Her expertise spans from cultivating strong vendor relationships to spearheading analytical teams dedicated to investigations. Rachel imparts her vast knowledge to a diverse audience, including investigators, security professionals, legal practitioners, financial experts, auditors, military intelligence personnel, and federal, state, and local agencies, enlightening them on the paramount practices in OSINT investigations and associated methodologies. As a Product Manager, she brings this expertise and deep understanding of the customer into product decisions to deliver real-world value.

About the authors.



John Mulligan

John Mulligan served as a senior executive leader at the Department of Defense for over 39 years managing national security, counterterrorism, and intelligence missions in complex, high risk environments.

As Deputy Director of the National Counterterrorism Center (NCTC), John developed government-wide strategic plans and operations to counter threats to the U.S. homeland. Prior to joining NCTC, he was responsible for the National Security Agency's (NSA) overall counterterrorism program. His role included integrating NSA capabilities with other U.S. government agencies to detect and disrupt terrorist threats around the world.

Mr. Mulligan began his career as an intelligence analyst and served in a variety of field and operations management positions. While serving overseas in his role as a Senior Representative, he championed development of data analytic technology to discover and disrupt terrorist networks. His many recognitions include being awarded the National Intelligence Sustained Superior Service Medal and the Presidential Rank Award, for Meritorious Executive Service.

A native of Chicago, John received his B.A. from the University of Notre Dame and an M.B.A. from the University of Florida.



John Adams

John Adams served 22 years as an FBI special agent, including in a variety of positions at FBI Headquarters and in several field offices. As Assistant Director of the Directorate of Intelligence, he directed intelligence collection, analysis, and sharing programs that enhanced interagency collaboration across the U.S. intelligence community. He also served as Deputy Assistant Director of the Counterterrorism Division and Special Agent in Charge of the Norfolk Field Office.

John has extensive experience investigating and overseeing terrorism and national security cases. John played a key role in the investigations of the 1998 U.S. Embassy bombing in Nairobi, the 2000 attack on the USS Cole in Yemen, and the 2003 Riyadh compound bombings, and he led the FBI's crime scene and evidence recovery operations at the Pentagon following the September 11th attacks.

Before joining the FBI, John served as a Special Agent and Forensic Scientist with the Tennessee Bureau of Investigation, where he conducted DNA analysis and crime scene investigations.

John holds a Bachelor of Science in Microbiology from East Tennessee State University and completed graduate studies in Forensic Anthropology at the University of Tennessee. John is a recipient of the Presidential Rank Award for Meritorious Service and the FBI Agents Association Award for Distinguished and Exemplary Service.

About the authors.



Rick Mercuri

Rick Mercuri has served as senior security executive at two of the largest U.S. banks. Rick is a trusted advisor to C-level executives and considered a thought leader with expertise in mitigating complex physical security risks and developing threat intelligence capabilities.

Among his many leadership roles, Rick was the Senior Director of Corporate Security for Santander US where he developed a comprehensive physical security program that included a 24/7 security operations center and an intelligence fusion center. He developed risk assessment methodologies, insider threat management capability, security training courses, and numerous programs, including workplace violence/active shooter and travel security.

Rick also served as the Senior Vice President and Head of Intelligence for RBS Citizens for the Americas region where he and his team managed external and insider threats impacting the organization. Rick took on several high-profile assignments including building a training and awareness team, implementing a global security model, and orchestrating the development and rollout of new security policies across the U.S. and Latin America.

Rick was appointed to advisory forums at Pennsylvania State University and Roger Williams University to contribute to the development of academic programs in global security and intelligence. Rick holds a bachelor's degree in criminal justice from Northeastern University and is a Certified Protection Professional (CPP).

We're here to help.

The framework in this guide runs on intelligence. Every phase, from assessing how your organization is perceived by threat actors to detecting the early signals that precede action, depends on seeing what is taking shape in the online spaces where grievances harden into intent.

Why Liferaft?

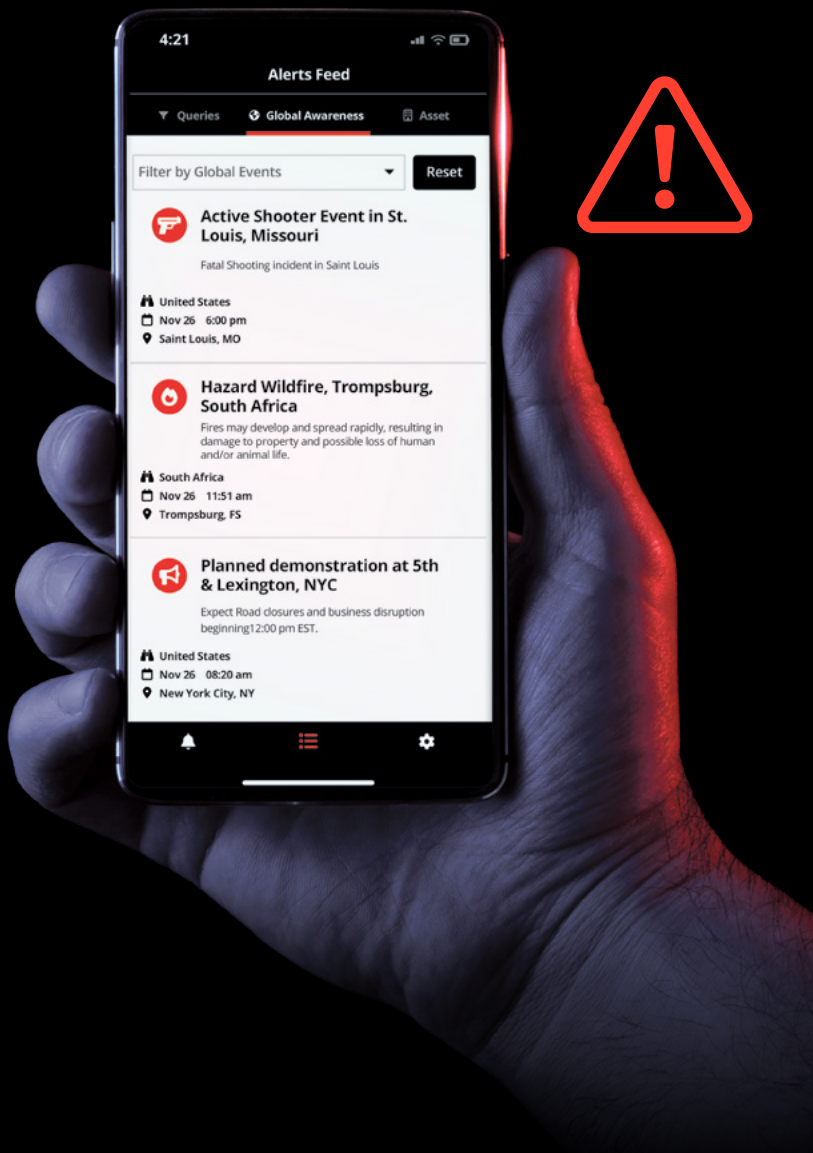
Liferaft is a decision-enablement platform that helps security intelligence teams turn open-source signals into credible, actionable intelligence. By connecting signals across surface, deep, dark, and fringe sources, it gives analysts visibility into the forums and echo chambers where political grievances first form, so rhetorical escalation is detected before it becomes physical risk.

AI-assisted workflows reduce noise and help teams distinguish protected expression from genuine warning signs, supporting the calibrated, proportionate responses this guide recommends. Identity resolution connects online personas to real-world actors, so executive protection and insider threat teams can escalate, stand down, and brief leadership with confidence.

Risk assessment
Standing collection against the actors, grievances, and locations your assessment surfaces

Early warning
Upticks in online organizing and counter-mobilization language, surfaced before demonstrations materialize

Executive protection
Protective intelligence on named principals, including digital footprint and exposure



liferaft
A Securitas company

Protect what matters.

Visit liferaftlabs.com/demo to schedule a discovery call.

Copyright ©2026 Liferaft. All rights reserved.