

SEC

SECURITY EXECUTIVE COUNCIL

A research and advisory firm



Executive Targeting Report: Analysis of Attacks on Corporate Executives from 2003-2025

An SEC Tier 1 Security Leader and Mercyhurst University Collaboration
January 2026 Public Safety Alert (redacted public release V1)

TABLE OF CONTENTS

- INTRODUCTION2**
 - Scope..... 3
 - Inclusion Criteria..... 3
 - Incident Typology..... 4
 - Limitations and Future Research 4
- EXECUTIVE SUMMARY.....6**
 - Incidents..... 6
 - Executives..... 6
 - Assailants..... 6
- BY THE NUMBERS7**
- EXECUTIVE CHARACTERISTICS8**
- ASSAILANT CHARACTERISTICS9**
- INCIDENT: OVERVIEW.....10**
- INCIDENT: LOCATION.....11**
- INCIDENT: PHYSICAL.....12**
- INCIDENT: PROTEST15**
- INCIDENT: CYBER17**
- CASE STUDIES18**
- CONCLUSION18**
- ACKNOWLEDGMENT18**
- ABOUT US.....20**
- CONTACT US.....21**

INTRODUCTION

The information contained in this report has not previously been released to the public. The startling increase in attacks from 2023-2025 has prompted this public version- in order to alert executives to this higher risk threat level.

The original executive targeting data set underlying this report was developed by a SEC Fortune 500 client security leader and their Protective Intelligence team, widely recognized for its analytic rigor and operational excellence. That team systematically identified and documented executive targeting incidents from 2003–2022 using open-source reporting drawn primarily from verified news media and public records.

The Security Executive Council (SEC) incorporated these findings into its 2023 State of the Industry Report on Executive Protection Programs as part of its commitment to confidential, collective knowledge-sharing across the SEC community, with support from Mercyhurst University’s Center for Intelligence Research, Analysis, and Training (CIRAT). To further strengthen and extend the work, Mercyhurst student analysts in the Business Intelligence & Innovation (BI²) Lab reviewed, validated, and expanded the dataset under SEC guidance.

Building on that foundation, the original authors continued to contribute subject-matter expertise by working directly with BI² Lab analysts to extend the executive targeting research through 2023–2025. This ongoing collaboration ensures the dataset remains current, methodologically sound, and operationally relevant, and the research will be maintained and advanced within the SEC’s BI² Lab going forward.

The purpose of this research is to provide a comprehensive assessment of historical and emerging threats directed at senior business leaders in the private sector. By analyzing incidents from 2003 through late-2025, this study delivers a data-driven perspective on how physical and cyber threats against corporate executives have evolved and intensified across global regions and industries.

This assessment draws from open-source reporting on targeted incidents involving corporate executives to support situational awareness for security and protective intelligence professionals. The findings help practitioners identify long-term threat patterns, evaluate risk exposure, and strengthen decision-making related to executive security and organizational risk posture.

Although the dataset spans more than two decades, a significant proportion of incidents occurred within the past five years, underscoring the growing visibility and vulnerability of business leaders. Threat activity shifted significantly following the December 2024 homicide of a Fortune 500 healthcare CEO, an event that significantly influenced public and corporate perceptions of executive-directed violence. For many executives, the event prompted reflection on their overall risk landscape and the potential vulnerabilities of their families and assets.

While this study's dataset does not directly measure or attribute changes in incident volume to the December 2024 attack, broader industry observations help contextualize its symbolic impact. The extensive and sustained media coverage of the attack elevated its visibility and influence within public discourse. In the months that followed, several incidents and online threats toward executives invoked the language or themes associated with the case. A broader sentiment also emerged across social platforms, where users expressed sympathy or justification for the assailant and framed the event as a form of resistance against perceived corporate greed or systemic injustice. These dynamics unfolded within a wider environment of heightened grievance expression, polarized discourse, and declining institutional trust.

This study addresses a critical gap in publicly available research on attacks against business executives. It provides operationally relevant insights that enable corporate security leaders, executive protection teams, and intelligence professionals to anticipate evolving risks, refine protective strategies, and strengthen resilience against emerging threat vectors.

Scope

This research identifies and analyzes physical and cyber incidents targeting corporate business leaders worldwide between January 1, 2003, and October 31, 2025, using open-source collection methods. Incidents were identified primarily through structured Boolean searches and keyword-based collection across global media reporting, law enforcement reporting, and other publicly available sources. Because data collection relied on search engines and artificial intelligence-assisted discovery of open-source reporting, incidents that existed only on social media platforms were not systematically captured. More than 50 variables were collected for each incident, grouped into three major categories: characteristics of the executive, characteristics of the assailant, and the circumstances of the incident.

Inclusion Criteria

The dataset includes incidents targeting senior corporate executives of any title or role, including but not limited to CEOs, COOs, CFOs, founders, presidents, and members of corporate boards. Family members and executive staff were included when they were clearly targeted as an extension of the executive, such as in kidnap-for-ransom situations.

Individuals whose prominence derives primarily from non-corporate domains, including celebrities, entertainers, journalists, influencers, athletes, judges, and politicians, were excluded. Incidents targeting corporations or brands collectively, without a direct executive focus, were excluded. Only incidents demonstrating a clear intent to target an identifiable individual in a corporate leadership position were analyzed. The dataset also excluded incidents involving lower-level or mid-level corporate employees, as well as altercations or personal disputes where an executive initiated an altercation or acted as an instigator, rather than being targeted because of their corporate role. These exclusions ensure that the dataset remains focused on intentional, role-driven targeting of senior business leaders.

Suspicious or unexplained deaths of business figures, such as those reported in Russia and other high-risk jurisdictions, were excluded due to limited verifiable evidence linking these incidents to deliberate targeting or identifiable assailants. Similarly, nonspecific threat behavior was excluded when it did not identify an individual executive. This includes threats directed only at a company's "senior executives" or "leadership," where no specific target could be reliably determined, even if the organization's executive roster was publicly available at the time of incident.

Incident Typology

Physical incidents include, but are not limited to, assassinations, kidnappings, assaults (violent and symbolic), robberies, stalking, physical surveillance, vandalism, and both violent and non-violent protests. Cyber incidents include examples in the digital domain such as death threats, impersonations, swatting, and account compromise. Hybrid incidents were also recorded when a case clearly involved both cyber and physical components, such as an online death threat followed by the assailant traveling to an executive's workplace.

Limitations and Future Research

This study relies on open-source reporting, which introduces inherent limitations. Despite comprehensive collection efforts, the constraints of open-source data and inconsistent global reporting standards mean the dataset should be viewed as a representative snapshot rather than a complete record of all incidents. Many incidents are never publicly disclosed due to corporate reputation concerns, legal considerations, or privacy restrictions, resulting in underreporting that is likely to reduce the observable volume of executive-targeted activity.

Many cases, particularly those overseas or covered in non-English media, were likely not captured, and the detail available across reports varied considerably. Incidents that did not result in harm or significant disruption may also be absent, creating a survivorship bias that skews reporting toward higher-impact events. Threats or attacks involving well-known companies or highly visible executives were more likely to be documented, potentially overrepresenting large public corporations and underrepresenting privately held or smaller firms. Despite these constraints, the dataset remains the most comprehensive open-source collection of attacks directed at executives to date and provides valuable insights

Information about offenders was especially limited; little is known about their criminal histories, mental health backgrounds, or prior threatening behaviors, and missing offender data further constrains the ability to analyze pre-incident indicators, pathways to violence, or escalation patterns. For non-fatal incidents, open-source accounts rarely clarify why attacks resulted in limited harm or whether security intervention played a role, an area that would benefit from deeper analysis in future research. It also remains unclear whether targeted executives had prior awareness of threats or potential actors through warnings or intelligence alerts, and in many cases the assailant's motive or intent could not be reliably determined from available information. Stock market impacts were similarly difficult to assess, as post-incident financial data was unavailable in most cases and broader market conditions frequently obscured any direct effects.

Despite these constraints, the dataset remains the most comprehensive open-source collection of attacks directed at executives to date and provides valuable insights for the executive protection and protective intelligence community. The findings can help organizations strengthen threat detection, inform proactive risk management, and refine protection strategies. Future research should address the identified information gaps by examining assailant profiles, pre-incident behaviors, and how digital activity now shapes physical threat behavior. This includes the growing pattern of individuals issuing threats or hostile communications online before attempting an in-person approach, the ways online exposure or compromised personal information can enable real-world targeting, and the increasing use of artificial intelligence tools to support reconnaissance and other preparatory actions. Understanding these intersections of technology, human behavior, and executive vulnerability will be key to advancing intelligence-led protection in the years ahead.

Public Release and Attribution Notice

This public version of the report is not intended for direct publication or posting to any website and is provided for limited informational use only. It is a redacted and summarized derivative of proprietary research developed and maintained by the Security Executive Council (SEC) through its Business Intelligence & Innovation (BI²) Lab at Mercyhurst University. Certain data sources, analytical methods, case details, and contributor identities have been removed or generalized to protect confidential sources, participating organizations, and ongoing research.

The findings are intended for informational and awareness purposes only and reflect aggregated trends derived from open-source analysis and SEC-governed research. This version may not be used to infer the security posture, risk exposure, or operating practices of any specific organization, nor should it be relied upon for operational, legal, or risk management decisions.

All rights to the underlying dataset, methodologies, and ongoing research remain with the Security Executive Council. Reproduction, redistribution, or commercial use of this material, in whole or in part, requires prior written authorization from SEC.

EXECUTIVE SUMMARY

Incidents

- A total of 424 incidents were reported. Of these, 85% involved physical activity, 14% were classified as cyber incidents, and 1% were categorized as hybrid incidents.
- Incident levels have continued to rise over the past two decades, with notable increases since 2023. As of October 31, 2025, the number of recorded incidents has already doubled the total reported for all of 2024, representing a 100% increase and marking the highest level on record even before year-end.
- 33% of incidents resulted in death or physical injury.
- Workplace and residence targeting have increased across physical incident types since 2020, while incidents at events have risen primarily due to protest activity.
- Targeting remains concentrated midweek. Violent incidents peak midweek and on Fridays, with higher frequency in the summer. Non-violent incidents occur most often early to midweek and show a pronounced peak in the spring, likely reflecting periods of increased executive visibility.

Executives

- 84% of attacks targeted male executives, but female executive targeting has increased since 2021, reaching record levels in 2025.
- CEOs remain the most targeted (64%) yet attacks on non-CEO senior executives are increasing significantly, showing a broader focus by threat actors.
- Executives in the technology and financial industries are the most frequently targeted, accounting for over one-third of all incidents.

Assailants

- Most assailants were strangers with no prior connection to the executive, but incidents involving current and former employees have become more common in recent years.
- Weapons were confirmed or suspected in 37% of incidents, with firearms present in 22%.
- Activism (38%) and criminal (36%) motives were the most common reasons for incidents, with personal grievances accounting for about 15%. Despite their lower frequency, incidents driven by personal motives were disproportionately dangerous, with 70% of assailants armed.



SECURITY EXECUTIVE COUNCIL

A research and advisory firm

BY THE NUMBERS

A Comparison of 2023 vs. 2025 Statistics

INCIDENTS

424 total incidents
313% increase from 2023

85% were physical
305% increase from 2023

54% occurred in the AMER region
370% increase from 2023

53% involved two or more assailants
308% increase from 2023

50% occurred in exec's home city
400% increase from 2023

46% occurred in the U.S.
356% increase from 2023

42% occurred during the day
375% increase from 2023

38% were motivated by activism
463% increase from 2023

CHARACTERISTICS

84% of executives were males
339% increase from 2023

76% of assailants were strangers
365% increase from 2023

64% of executives were CEOs
327% increase from 2023

37% of assailants used weapons
189% increase from 2023

33% of targets were killed or injured
150% increase from 2023

32% of executives were non-CEOs
225% increase from 2023

18% of assailants had a work nexus
250% increase from 2023

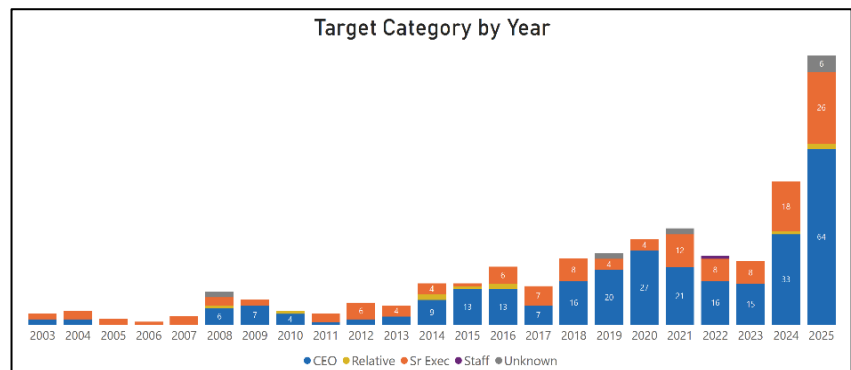
17% of executives were in tech
340% increase from 2023

EXECUTIVE CHARACTERISTICS

Target Demographics and Executive Positions

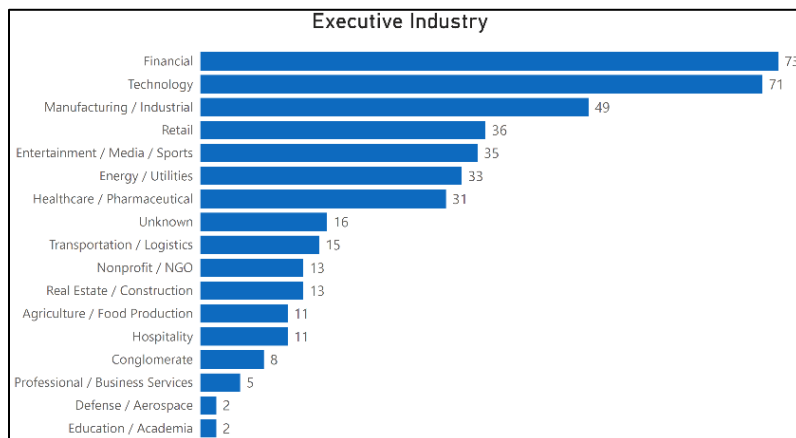
Among cases with known demographic data (93%), most targeted executives since 2003 were male (84%), while females accounted for approximately 9%. Although female executives remain a smaller share of targets, incidents involving them have risen by 100% between 2021 and 2025. While CEOs represented the largest share of targeted individuals (64%), there has been a marked increase in incidents involving non-CEO senior leadership roles, including a 225% increase since 2023. This shift suggests a broader focus by threat actors on senior leaders beyond the CEO, including presidents, COOs, CFOs, board members, and other senior roles, who accounted for 32% of all targets.

Relatives and executive staff were also affected in a small number of cases (3%).
Additional analysis in full report.



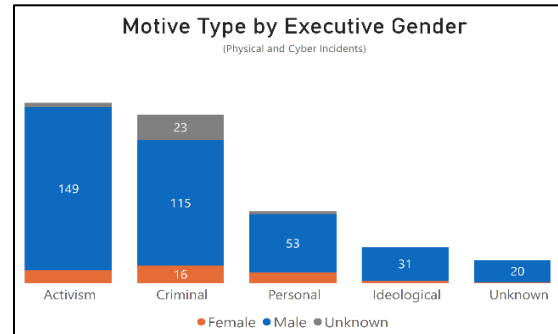
Executive Industry

The most frequently targeted industries were financial (17%), technology (17%), and manufacturing/industrial (12%), followed by retail (8%), entertainment/media/sports (8%), energy/utilities (8%), and healthcare/pharmaceutical (7%). Beyond these leading industries, incidents were distributed across a wide range of additional industries, such as nonprofits, food production, hospitality, and education, reflecting the broad reach of executive targeting.



Gender-Based Targeting Patterns

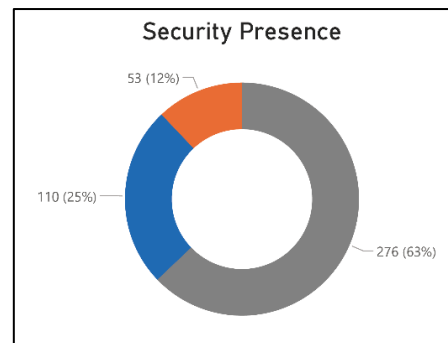
Incidents involving female executives were most likely to occur at their residences (64%), compared with 44% for males, and were less frequent in workplaces, public areas, or corporate event settings. Female executives also experienced higher proportions of physical attacks (34%), protests (29%), and kidnappings (17%). Male executives were also frequently targets of these incident types, but they were affected by a broader range of behaviors overall, such as property crime, impersonations, and pre-operational activity. Regarding assailant motive, females were most often targeted for criminal (39%), activism-related (29%), and personal (24%) motives, while males were primarily targeted in activism-related incidents (40%), followed by criminal motives (31%) and smaller shares of personal or ideological drivers.



Tactics for physical approach and attacks varied by gender and method of attack. Walk-up and direct attacks were the most prevalent for both female (71%) and male (75%) executives. **Additional analysis in full report.**

Security Presence

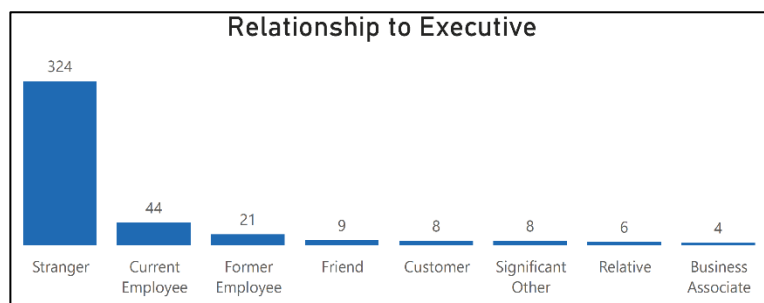
Analysis in full report.



ASSAILANT CHARACTERISTICS

Assailant Profile

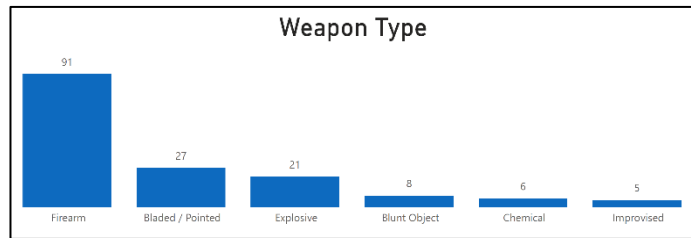
Information on assailants, those who carried out the incidents, was less consistently available than data on executive characteristics, primarily due to limited reporting standards and the low rate of criminal apprehension. Nearly half (43%) of assailants' genders were unknown, while 34% were identified as male, 19% involved groups comprising both males and females, and 4% were female. Regarding the assailants' relationship to the target, 76% were classified as strangers, while 18% had a workplace connection, such as a current or terminated



employee. Most incidents involved multiple individuals: 53% included two or more, 27% were carried out by a lone actor, and 20% involved an unknown number of participants.

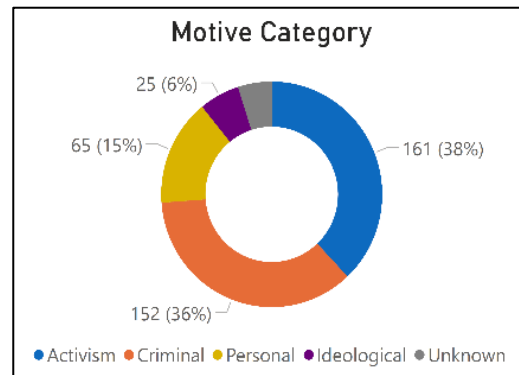
Weapon Type

Assailants were armed in 37% of incidents, unarmed in 36%, and unknown in 27%. Of the 158 incidents in which a weapon type was identified, firearms were most frequently used (22%), followed by bladed/pointed weapons (6%), explosives (5%), blunt objects (2%), and chemical or improvised weapons (1% each).

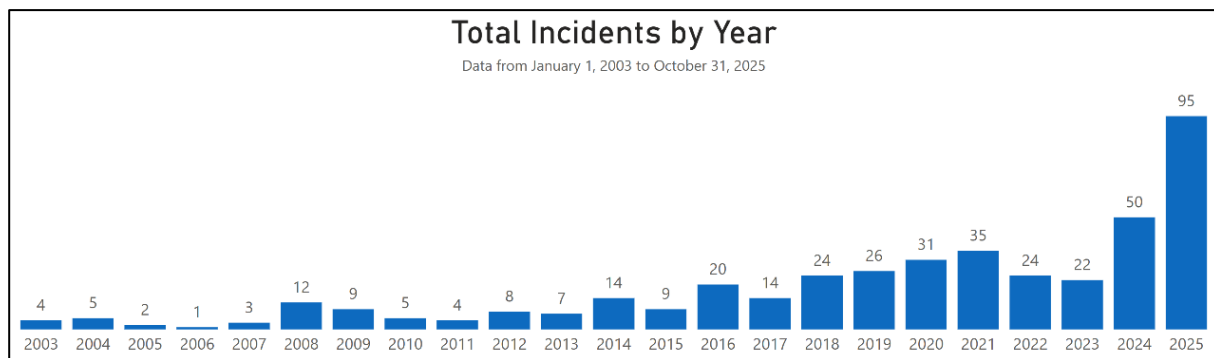


Motives and Violence Drivers

Although activism was the most common motive overall, the pattern shifts when incidents are separated by violence level. Violent incidents were driven primarily by criminal motives (52%) and personal grievances (28%), while non-violent incidents were largely linked to activism (66%), consistent with the demonstration-based nature of protest activity. Regarding assailant composition, among confirmed cases, 73% of activism-related incidents involved groups (defined as two or more individuals), whereas criminally motivated cases showed a mix of lone actors (23%) and groups (47%). Personal-motive incidents occurred primarily at an executive’s residence or workplace (69%), and in these cases, nearly 80% involved an armed assailant, indicating higher potential for severe outcomes.



INCIDENT: OVERVIEW



Incident Classification

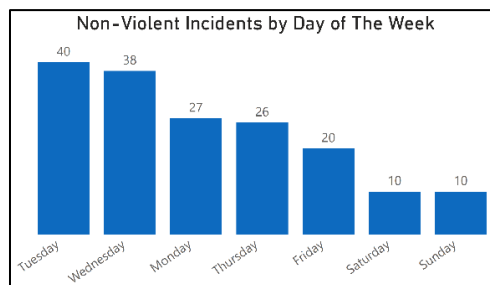
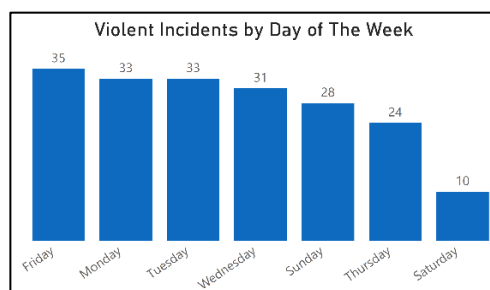
A total of 424 incidents targeting executives were identified between January 1, 2003, and October 31, 2025. Incidents were categorized into physical, cyber, and hybrid types. Physical incidents accounted for 85% of all cases, cyber incidents for 14%, and hybrid incidents for 1%. Hybrid cases were defined as incidents where it was confirmed the threat actor used both digital and physical components, such as conveying a death threat online and then making a physical approach.

Long-Term Trend

Overall, the data shows a clear upward trend over the past two decades, with more consistent growth beginning after 2015. After a temporary decline in 2022 and 2023, incidents began to rise again in 2024, culminating in a sharp increase in 2025, with 95 cases recorded despite the year's data being incomplete. During the 2022–2023 period, protest and cyber-related incidents decreased, while physical attacks and kidnapping cases remained stable. The increase in 2024 was driven largely by activism-related incidents, including protests and property crime.

Temporal Patterns

Incidents occurred most frequently during the work week, with non-violent cases peaking on Tuesdays and Wednesdays and declining over the weekend. Violent incidents showed a different pattern, reaching their highest levels on Fridays, indicating an end-of-week escalation among higher-risk assailants. Seasonally, spring and Q1 recorded the most incidents, while fall and Q3 had the lowest. March produced the highest number of cases, with December, January, and April also showing elevated activity. Non-violent incidents were most common from January through May, whereas violent incidents peaked in December and again during the summer. Overall, the data indicates that threats cluster earlier in the year, likely reflecting periods of increased executive visibility and public engagement.

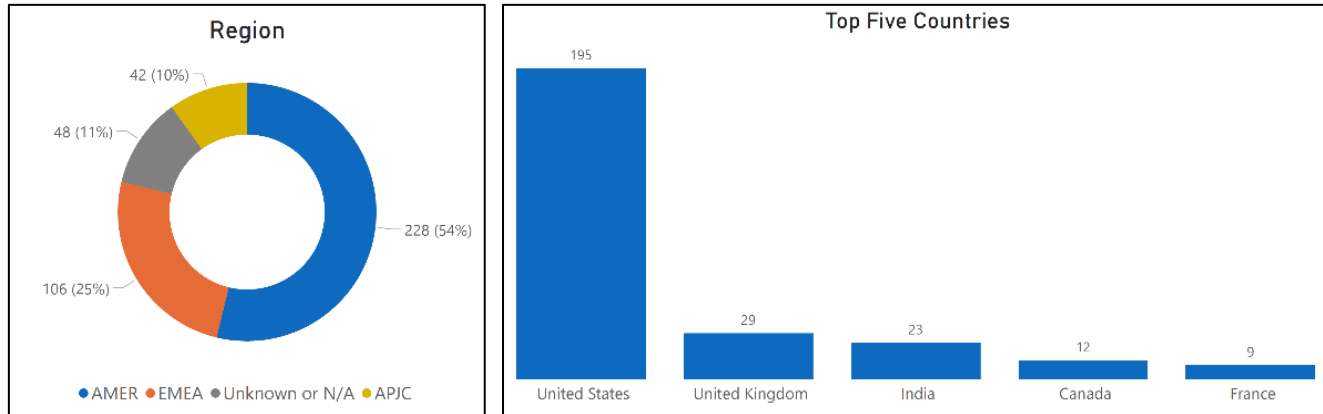


INCIDENT: LOCATION

Geographic Distribution

Based on available location data, most incidents occurred in the AMER region (54%), followed by EMEA (25%) and APJC (10%), while 11% were categorized as cyber-based with no defined geographic location. Within the AMER region, the United States accounted for 46% of incidents. Across the over 50 countries where incidents were recorded, the United States (195 incidents) ranked highest by a wide margin, followed by the United Kingdom (7%), India (6%), Canada (3%),

and France (2%). The dominance of the United States highlights its position as the primary location for executive targeting, representing nearly half of all recorded incidents worldwide.



Location Setting

Since 2020, workplace incidents and corporate event related incidents have seen the sharpest rise, highlighting a substantial escalation across corporate environments. Most event incidents occurred in the United States, while workplace incidents were more dispersed, with the United Kingdom second to the United States. **Additional analysis in full report.**

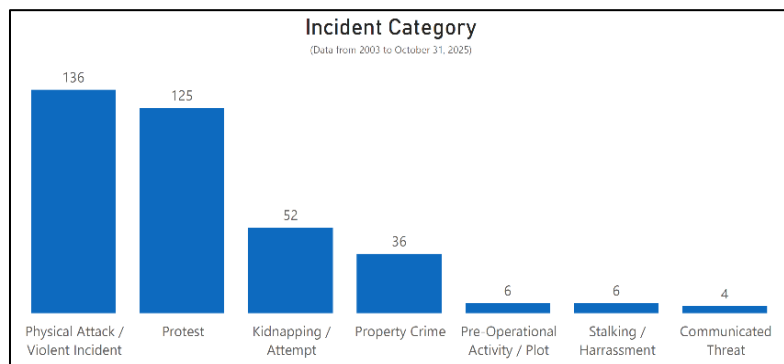
INCIDENT: PHYSICAL

Key Characteristics

Focusing on physical incidents, which accounted for 85% of all cases, the most common incident type was physical attack/violent incident (37%), including assaults, shootings and stabbings. Among these cases, 75% were carried out through ambush/walk-up tactics, while 8% involved drive-by shootings. Protest activity, both violent and non-violent, accounted for an additional 34% of incidents, meaning that violent attacks and protests together represented the majority of all recorded cases. Kidnapping cases accounted for a smaller share (12%). **Additional analysis in full report.**

Incident Sub-Types

Analysis in full report.



Incident Impact

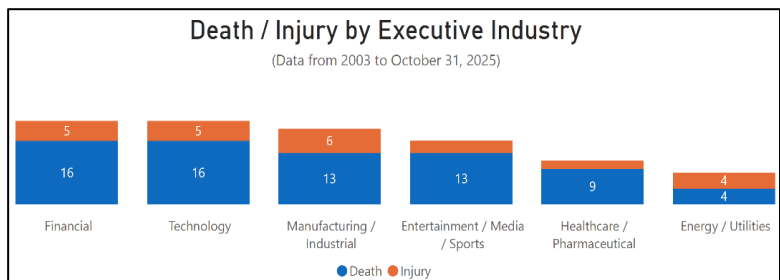
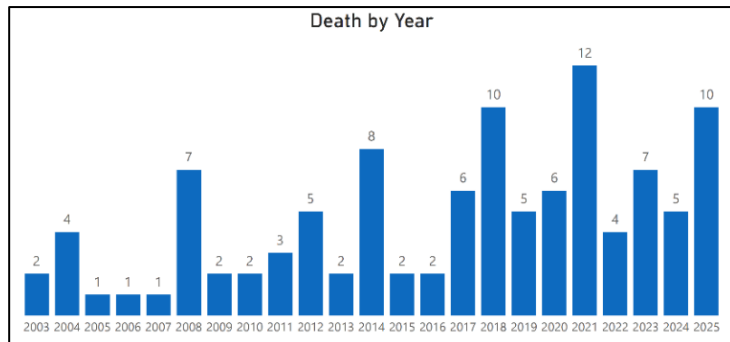
Incident impact was categorized into five primary types: disruption (47%), death (29%), injury (10%), property damage (10%), monetary loss or data compromise (3%), and missing persons unaccounted for after kidnapping (1%). These categories were used to capture the full range and severity of outcomes. While physical incidents represent the most acute form of harm, nonlethal events, particularly those involving disruption, occur more frequently and carry lasting impacts. Nearly half (47%) of physical incidents caused operational disruption, such as prompting law enforcement response, forcing an executive to physically flee, or affecting business operations.

Lethal and Injury-Related Incidents

Across all physical incidents, 33% resulted in death or injury. Fatal attacks have remained elevated since 2017, with notable peaks in 2018 and 2021, indicating a sustained pattern of lethal incidents in recent years. Among these fatal events, most assailants were either strangers (56%) or had a workplace connection (24%). Assailants with personal motives were the most likely to use weapons, indicating that grievances continue to play a meaningful role in armed attacks.

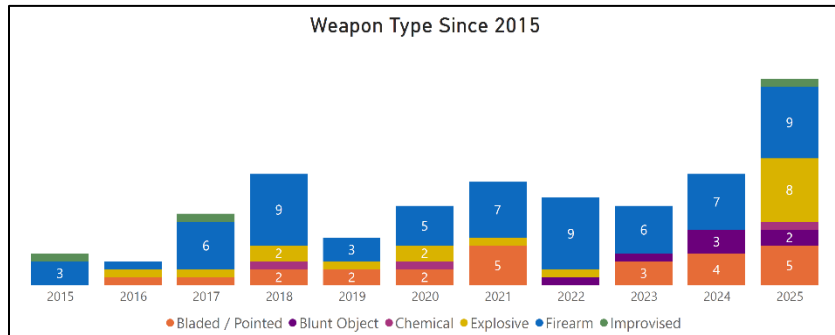
Among industries with the highest volumes of serious incidents, the likelihood of fatal versus non-fatal outcomes varied. Fatal attacks predominated in healthcare/pharmaceutical (82%), entertainment/media/sports (81%), technology (77%), and financial (76%), while manufacturing/industrial incidents showed a higher proportion of injuries (38%). Although incident volume was lower, energy/utilities was the only major industry with an even split between fatalities and injuries. Across industries, assailants with no prior connection to executives were most common in both fatal and injury incidents; however, technology and manufacturing/industrial sectors exhibited a higher incidence of attacks involving assailants with workplace ties, including current or former employees.

Additional analysis in full report.



Weapon Type

Firearms remained the most prevalent weapon and primary driver of fatal outcomes, with overall weapon involvement rising after 2020 and bladed/pointed weapons appearing more frequently in recent years. Other weapon categories remained limited in volume, though recent years reflect a broader mix, driven primarily by episodic use of explosives and the recent emergence of blunt objects. Regionally, incidents in AMER remained predominantly firearm-driven, while EMEA exhibited higher use across multiple weapon types, including firearms, explosives, and bladed/pointed weapons.

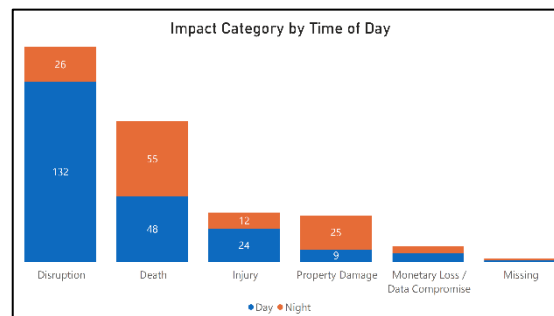


Temporal and Location Patterns

Although physical incidents have collectively trended upward across regions, the most substantial increases occurred between 2023 and 2025, with EMEA increasing by 500% and AMER by 330%. In EMEA, this escalation was driven primarily by kidnappings and protests, supplemented by recent increases in incident sub-types such as arson, kidnap-for-ransom, and surveillance. In AMER, growth was concentrated in vandalism, shootings, arson, and protest-related sub-types, while APJC exhibited no meaningful changes.

Incidents resulting in property damage occurred mostly at night. Armed incidents occurred more frequently at night across most regions; however, in the United States, day and night occurrences were nearly evenly divided. Russia and Nigeria recorded the highest proportions of armed incidents (100%), followed by India (70%), and South Africa (67%).

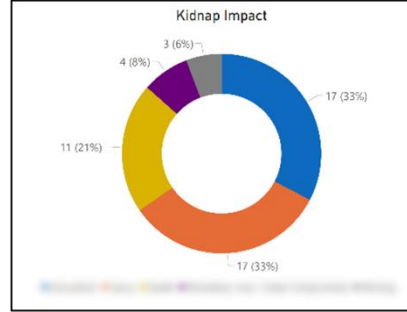
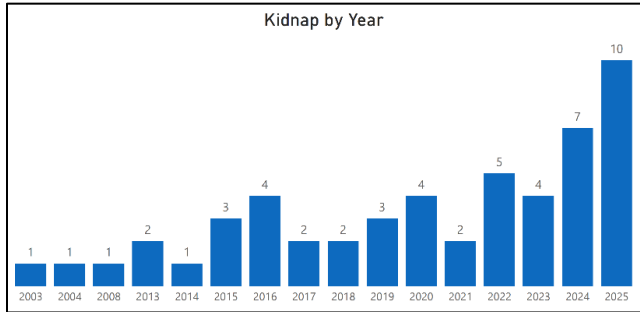
Additional analysis in full report.



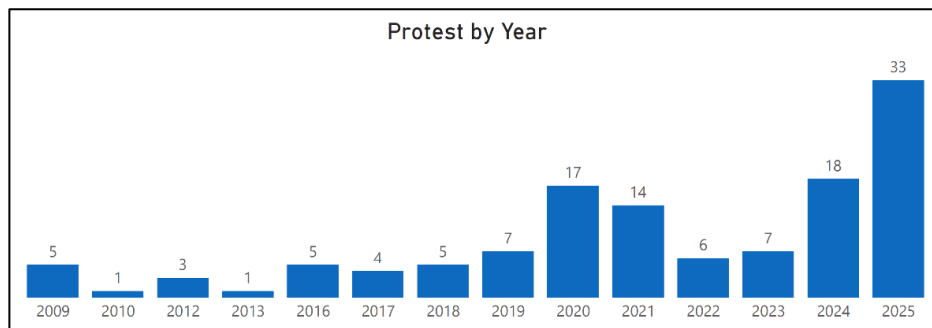
Kidnapping Trends

Given the relevance of kidnapping risk to executive protection, the following section provides additional insight into kidnapping incidents. Since 2003, kidnappings have remained persistent, characterized by low counts and moderate year-to-year variation through the mid-2010s. A gradual increase became evident beginning around 2015, followed by a more pronounced rise after 2020. The sustained growth from 2022 onward, reaching peak levels in 2024 and 2025, indicates a clear and accelerating resurgence rather than a stable or purely incremental trend.

Additional analysis in full report.



INCIDENT: PROTEST



Key Characteristics

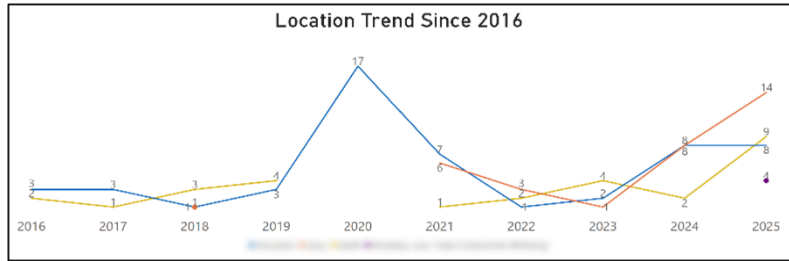
Protest activity targeting executives has increased over time, reaching a record 33 incidents in 2025 as of October 31. These totals reflect only incidents categorized as protests; activism-motivated events that manifested as other sub-types (such as property crime or assaults) were captured separately. For example, a single activist throwing an object at an executive in public would be classified as a symbolic assault rather than a protest. When all physical, cyber, and hybrid incidents are considered, activism-motivated cases total 161, accounting for 38% of all incidents. This provides a more comprehensive view of activism-related activity beyond protests alone.

Drivers of Protest Activity

Across the full timeline, the data shows a clear shift in what drives protesters to target corporate leaders. In the late 2000s through mid-2010s, protests were dominated by classic workplace and economic grievances such as wages, unionization, layoffs, and healthcare costs, with environmental actions present but generally tied to specific projects rather than broad climate narratives. Beginning around 2018–2020, the scope widens: climate activism accelerates, anti-billionaire sentiment grows, and technology-related frustrations emerge, including concerns about platform moderation and workplace surveillance. The year 2020 marks the first major spike in protest volume, shaped by COVID-19-era economic pressure and social-justice mobilization, and it serves as the inflection point for the more diverse protest landscape that follows.

Shift Toward Geopolitical and Identity-Based Activism

Beginning in 2022, activism increasingly centers on geopolitical issues, including Israel-Palestine, Russia-Ukraine, and corporate involvement in global conflicts, while also becoming more personalized in its focus on high-visibility technology leaders. After a brief decline, protest activity rises again starting in 2023, driven by intensified climate and energy activism, concerns related to artificial intelligence and automation, and a broader mix of geopolitical and U.S. domestic political issues. The overall trend reflects a shift from primarily workplace-driven grievances to a politically complex, globally networked, and increasingly identity-focused environment in which individual executives, not just institutions, serve as strategic targets. At the same time, protests at workplaces and corporate events continue to grow, underscoring activists' preference for predictable, high-visibility locations that maximize operational disruption and media impact.



Temporal and Location Patterns

Geographically, protest activity is heavily concentrated in AMER and EMEA, which together account for 96% of all cases. In AMER, the United States accounts for 97% of protests, spanning 18 states. Activity clusters around major economic hubs, with California (23%), New York (19%), Washington (9%), Texas (5%), and the District of Columbia (5%) representing the highest concentrations. In EMEA, the United Kingdom leads with 57% of protests, followed by Germany and Italy at 14% each. **Additional analysis in full report.**

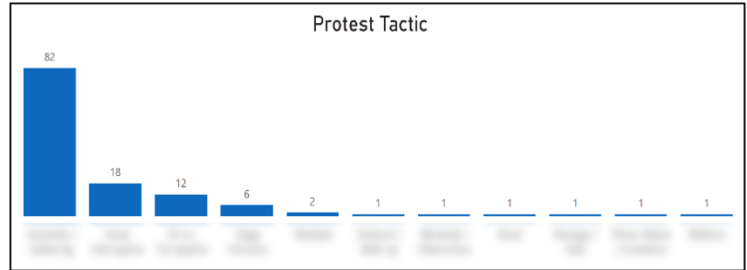
Executive Role and Industry

Protest activity remains highly CEO-focused, with 86% of incidents directed at CEOs and 14% at senior executives. Across industries, the most notable increase since 2024 occurred in technology, increasing from five to 12 incidents. The energy/utilities industry also shows a clear upward trajectory, growing from one incident in 2020 to five in 2025. These shifts indicate that while most industries show limited movement, technology and energy/utilities industries are becoming increasingly prominent.

Protester Profiles and Tactics

While most protester affiliations are unknown, 74% of activists are classified as strangers or unknown, 25% have a confirmed workplace connection.

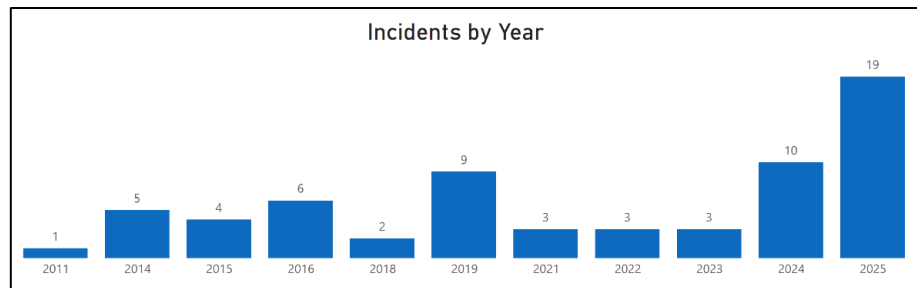
Additional analysis in full report.



INCIDENT: CYBER

Key Characteristics

Cyber-related incidents targeting executives account for 14% of all recorded cases, first appearing in 2011 with spikes in 2016 and 2019. Following a period of lower activity between



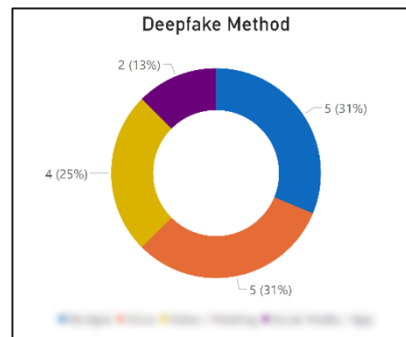
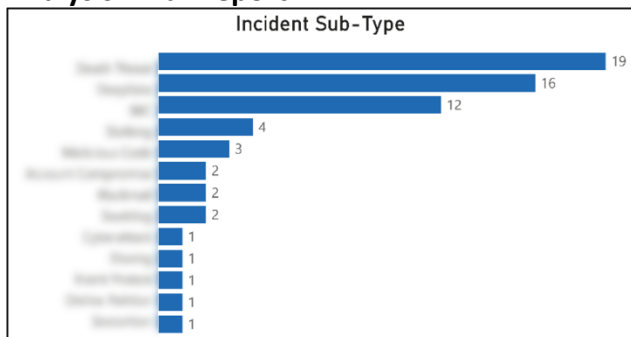
2021 and 2023, incident volume increased in 2024 and reached its highest level to date in 2025. This escalation reflects a growing and increasingly capable digital threat environment. A major contributor to the 2025 rise was the surge in impersonations, which expanded significantly after 2023 with the widespread availability of artificial intelligence tools that lowered both the skill and cost barriers for impersonation-based attacks. This pattern aligns with broader technological shifts shaping the current cyber landscape.

Industry

Technology executives were the most frequently targeted, accounting for 34% of all cyber incidents. Manufacturing/industrial (14%), financial (9%), entertainment/media/sports (8%), and healthcare/pharmaceutical (8%) followed, while all other industries represented a comparatively small share of cases.

Incident Sub-Types

Analysis in full report.



Threat Actor Profiles and Tactics

Analysis in full report.

Motive and Impact

Motive patterns were heavily concentrated around financial gain, which accounted for 66% of cyber incidents. **Additional analysis in full report.**

Cyber-to-Physical

In four cases, cyber indicators directly preceded physical approaches, demonstrating a clear linkage between online threat activity and real-world mobilization. **Additional analysis in full report.**

CASE STUDIES

Analysis in full report.

CONCLUSION

Attacks on corporate executives continue to rise, with CEOs remaining the most frequently targeted and a growing share of incidents now directed at non-CEO senior leaders. Recent patterns indicate that non-CEO executives are also increasingly exposed to kidnapping risk, potentially reflecting greater accessibility, expanded operational visibility, or growing strategic relevance within organizations. As threat actors adapt to evolving global, social, and technological conditions, executive protection and protective intelligence teams must anticipate shifts in targeting behaviors, tactics, and escalation pathways.

Protests and activism-driven incidents have become more common, often accelerating alongside broader waves of global grievance expression. Recent cases linked to pro-Palestine demonstrations, climate change activism, anti-billionaire sentiment, and other anti-corporate movements illustrate how socio-political pressures can quickly translate into executive-level risk. These dynamics highlight how executives may emerge as focal points for symbolic opposition, particularly during periods of heightened geopolitical tension or social unrest.

Recent patterns also demonstrate that executive risk is not evenly distributed across demographics or roles. As executives become more visible through public engagements and online presence, their exposure to both physical and digital threats continue to grow.

ACKNOWLEDGMENT

The Security Executive Council extends its appreciation to the project team and its academic partners at Mercyhurst University for their collaboration in the development of this report. The work was informed by a contributing subject matter expert, a senior protective intelligence professional from a Fortune 500 technology company, who provided domain knowledge and methodological guidance to support analytical rigor and alignment with practical corporate

security considerations. These combined contributions strengthened the relevance and quality of the insights presented herein.

ABOUT US

About the Contributing Subject Matter Expert

The Contributing Subject Matter Expert is a senior Protective Intelligence professional from a Fortune 500 technology company with extensive experience in executive protection, threat assessment, and open-source intelligence. Their background spans corporate protective intelligence, law enforcement analysis, and behavioral research, bringing a unique blend of operational and analytic expertise.

Through this collaboration, they provided domain knowledge and methodological guidance to the BI² Lab analysts, helping ensure the executive targeting research remains rigorous, current, and aligned with real-world corporate security practice.



The BI² Lab is a collaboration between the SEC and Mercyhurst University. The BI² located at Mercyhurst creates and leverages intelligence-driven security risk research and tools to assist corporate security leaders in identifying and communicating information that is relevant to private-sector business.

<https://www.securityexecutivecouncil.com/insight/program-best-practices/secs-business-intelligence-and-innovation-lab-now-open-2030>



The SEC is the leading research and advisory firm focused on security risk mitigation solutions. Having worked with hundreds of companies and organizations, we have witnessed the proven practices that produce the most positive transformation. Our subject matter experts have deep expertise in all aspects of risk mitigation strategy; they collaborate with those that have security responsibilities to transform programs into more capable and valued centers of excellence. www.securityexecutivecouncil.com



The Security Leadership Research Institute (SLRI) is dedicated to providing independent and actionable research to the security and risk community. The SLRI was formed as a result of the need by the security industry to document the entire spectrum of risk mitigation and security through research.

<https://securityexecutivecouncil.com/research/security-leadership-research-institute>



Mercyhurst University; known as a dynamic university that builds community and advances the common good as they promote wisdom, mercy, and respect in all its engagements. They educate and inspire diverse learners in an environment where faith and reason flourish together for meaningful lives, dignified work, and leadership in service toward a just and loving world.

<https://www.mercyhurst.edu/>

CONTACT US

Email us at contact@secleader.com

For a faster response, [please fill out this form.](#)

Call us at +1 202 730 9971