The Analysis Deficit:

Why Identifying Threats Is Not the Same as Understanding Them

Executive Summary

The Programmatic Context

Corporate security programs are expanding at an unprecedented pace. The share of S&P 500 companies providing executive security perquisites rose 27.8% between 2023 and 2024, and a further 12.8% in 2025 — with median spending more than tripling from 3,068 in 2021 to 30,468 in 2025. Chief security officers are authorizing larger budgets, building larger teams, and deploying monitoring infrastructure at a pace that reflects genuine organizational alarm.

The Data and Its Limits

This most recent wave of expansion was arguably sparked by a single incident and driven by a single research finding. In January 2026, the Security Executive Council (SEC) — a research and advisory firm — and Mercyhurst University's Business Intelligence and Innovation Laboratory published the most comprehensive open-source dataset of executive targeting incidents assembled to date, covering 424 incidents from 2003 to 2025. The SEC/Mercyhurst report documents a 313% increase in incidents between 2023 and 2025. What that figure cannot establish is whether it reflects a genuine rise in incident frequency or a rise in media visibility following the December 2024 homicide of a Fortune 500 healthcare CEO — a distinction the report's own authors acknowledge cannot be resolved with available data. Anecdote and headlines reach executive offices and boardrooms far more easily than rigorously analyzed data. That asymmetry is at the center of this paper's argument.

The Accepted Causal Chain

A parallel interpretive narrative has connected the rise in executive targeting to generalized social disorder — workplace incivility, anecdotal accounts of violent outbursts, road rage, declining civic norms — through a causal chain drawn from broken windows theory (1982). That causal chain is not advanced by the SEC/Mercyhurst report, is not supported by the report's own findings, yet is producing organizational responses disproportionate to what the evidence warrants. This narrative has been actively amplified in trade publications and security industry media, lending it an authority the underlying evidence does not support.

What is Broken Windows Theory?

Broken windows theory, introduced by criminologists Wilson and Kelling (1982), holds that visible signs of disorder — minor infractions, vandalism, unchecked incivility — signal that social norms have eroded, encouraging progressively more serious misconduct. Applied to corporate security, the argument is that deteriorating everyday behavior is a leading indicator of escalating violence. The theory has been influential but is also extensively critiqued for conflating correlation with causation and overlooking structural drivers of crime.

What the Data Actually Shows

The SEC/Mercyhurst report's own protest data tells a more analytically coherent story. The drivers of activism-motivated incidents stem from structural economic grievance: income inequality, pandemic-era dislocation, declining institutional trust. CEO compensation grew 1,094% from 1978 to 2024 while typical worker compensation grew 26%. Mancur Olson's collective action framework explains why this produces targeted rather than diffuse protest: named executives at named corporations are tractable — meaning identifiable and operationally approachable as collective action targets — in ways that diffuse institutions are not. The spend on executive protection may be rational. The shape of it — built on an undemonstrated causal chain — is not.

Three Disciplines, One Conflation

Executive protection responds to threats. Protective intelligence adds proactive threat assessment — but remains fundamentally investigative, asking subject-centric questions: is this person a threat to our principal? Intelligence and conflict analysis ask a structurally different question: what conditions are generating threats, and how are they evolving? Reactive detection, however sophisticated, is structurally incapable of comprehensive prevention. Only structural analysis operates upstream of the pathway entirely — asking not who is approaching, but why the approach is becoming more likely. The overarching risk intelligence field is actively navigating this tension. The question is whether it resolves toward rigor or convenience.

The Programmatic Consequence

When the wrong causal model drives program design, the incivility-to-violence narrative, accepted uncritically, produces threat models in which employee and civilian frustration (admittedly expressed at times in a reprehensible manner) becomes a risk signal — justifying extensive technology and personnel investments to drive workforce surveillance programs whose evidentiary foundation is incongruent with the organization's actual risk profile. It is worth acknowledging that the rapid expansion of executive protection and protective intelligence programs represents significant commercial opportunity for vendors, consultants, and service providers — a dynamic that does not make the underlying concern less real, but does warrant scrutiny of the causal frameworks being used to justify the investment.

The Case for Strategic Risk Intelligence

This paper calls for analytical standards commensurate with the organizational consequences of the conclusions being drawn. A risk intelligence function that supplements and provides greater depth to protection programs — informing decision-makers who can act on root causes, closing gaps across the enterprise, and earning its place not as a cost center, but as a driver of genuine organizational resilience.

A Note on Scope: What This Paper Is and Is Not Arguing

This paper is NOT arguing that:

- Executive targeting incidents are not increasing, or that the risk is not real
- The SEC/Mercyhurst report lacks value — it is the most comprehensive dataset of its kind
- Executive protection programs are unnecessary or should be reduced
- Protective intelligence programs serve no legitimate purpose
- Corporate security professionals are acting in bad faith

This paper IS arguing that:

- The causal chain connecting workplace incivility to executive-targeted violence is asserted, not demonstrated by the SEC/Mercyhurst report
- Open-source incident data cannot distinguish a genuine increase in events from an increase in their media visibility
- The SEC/Mercyhurst report's own protest data points toward structural economic grievance as the more analytically coherent explanation
- Protective intelligence, however sophisticated, is investigative rather than analytical — asking who is threatening our principal, not why the population of potential threat actors seems to be growing
- The spend on executive protection may be rational; the shape of it — built on unverified causal assumptions — is not
- The field's analytical standards should match the organizational consequences of its conclusions

The SEC/Mercyhurst Report and What It Actually Says

In January 2026, the Security Executive Council (SEC) — a research and advisory firm focused on corporate security risk — and Mercyhurst University's Business Intelligence and Innovation Laboratory (BI² Lab) published the Executive Targeting Report: Analysis of Attacks on Corporate Executives from 2003–2025 (hereafter the SEC/Mercyhurst report). The report represents a genuine contribution to the field — the most comprehensive open-source collection of executive targeting incidents assembled to date, covering more than 50 variables per incident across 424 documented cases spanning over two decades. Its scope is significant. Its limitations section is admirably candid.

The SEC/Mercyhurst report's dataset relies entirely on open-source collection — structured Boolean searches across global media reporting, law enforcement records, and other publicly available sources. Incidents are likely significantly underreported. Many cases overseas or covered in non-English media were probably not captured. Threats or attacks involving well-known companies and highly visible executives were more likely to be documented than those involving smaller or privately held firms. The findings, the report states explicitly, should be treated as a representative snapshot rather than a complete record.

Something is changing in the threat environment facing corporate executives. Protest activity targeting individual business leaders has reached record levels. Activism-motivated incidents now

reflect a politically complex, globally networked landscape. These are meaningful observations. The problem is not the data itself, but rather what risk intelligence teams are doing with it. Those caveats matter enormously and, in many situations, did not survive the translation from analysis to organizational practice (specifically: open-source reliance, likely underreporting of incidents, overrepresentation of high-visibility executives, and the inability to control for media coverage effects following the December 2024 assassination).

The Coverage Effect: What the SEC/Mercyhurst Report's 313% Increase Actually Tells Us

The SEC/Mercyhurst report's most cited finding is a 313% increase in total executive targeting incidents between 2023 and 2025. That figure has traveled widely since the report's January 2026 release — appearing in briefings, board presentations, and program justifications across the corporate security industry — and is treated, in practice, as evidence of a genuine surge in the frequency of attacks on business leaders. A critical dynamic underlies this pattern: anecdote and alarming headlines reach executive offices and shape organizational decisions far more readily than rigorously analyzed data. The 24-hour news cycle amplifies incident reports without context, and trade publications promote causal narratives that compress complex findings into actionable-sounding conclusions. The result is a policy environment in which alarm precedes evidence.

The SEC/Mercyhurst report itself is more careful. Open-source datasets are structurally vulnerable to ascertainment bias: the systematic underdetection of incidents that fall below a shifting threshold of public visibility. The report acknowledges that the December 2024 homicide of a Fortune 500 healthcare CEO significantly influenced public and corporate perceptions of executive-directed violence, and that several subsequent incidents invoked the language or themes associated with that case. The report then states explicitly that the dataset does not directly measure or attribute changes in incident volume to that event. No control for this effect exists. Organizations making consequential decisions about program investment, staffing, and workforce surveillance are doing so on the basis of a number whose importance has not been established with the precision the field is attributing to it.

The Accepted Causal Chain: What the SEC/Mercyhurst Report's Protest Data Actually Shows

In the period following the SEC/Mercyhurst report's release, a parallel narrative emerged in corporate security circles — one that the report itself does not advance, but which has become inseparable from how its findings are being interpreted and applied. That narrative connects the rise in executive targeting to a broader deterioration in social behavior: workplace incivility, parental misconduct at sporting events, passenger disruptions on commercial aircraft. The argument, drawn from broken windows theory (1982), is that generalized social disorder is

migrating upward — that rudeness in common spaces is a leading indicator of violence threatening executives. This framing invites a direct challenge: the causal chain it asserts has not been demonstrated, and by locating the cause in generalized social disorder rather than specific structural conditions, it closes off the explanatory alternatives most likely to produce actionable insight.

This narrative has been actively promoted in trade and industry media. Security Info Watch has published pieces framing workplace incivility explicitly as a security risk requiring behavioral intelligence and early-warning detection programs. Allied Universal's 2025 World Security Report characterizes the executive threat environment as driven by "social unrest, misinformation and digital radicalization" — connecting ambient social conditions to targeted violence without establishing the causal mechanism. Each of these sources reflects the work of serious practitioners. The concern is not their intent but the analytical leap: the consistent presentation of correlation as cause, amplified by a media environment that rewards alarming conclusions over methodological nuance. (See broken windows theory definition in the Executive Summary.)

What the SEC/Mercyhurst report's protest data actually shows is something considerably more specific and more structurally coherent. It documents a clear and traceable evolution in the drivers of activism-motivated incidents over two decades. In the late 2000s through the mid-2010s, protest activity targeting executives was dominated by classic economic grievances — wages, unionization, layoffs, healthcare costs. Beginning around 2018 to 2020, the scope broadened: climate activism accelerated, anti-billionaire sentiment grew, and technology-related frustrations emerged. The year 2020 marked the first major spike in protest volume, shaped by pandemic-era economic pressure. By 2022, activism had shifted further toward geopolitical grievances and domestic political polarization. The SEC/Mercyhurst report's own conclusion captures this trajectory: the overall trend reflects a shift from primarily workplace-driven grievances to a politically complex, globally networked environment in which individual executives serve as strategic targets. That is not a broken windows story. That is a political economy story.

The drivers of activism-motivated incidents stem from income inequality, pandemic-era economic dislocation, declining institutional trust, and a growing perception that corporate leaders operate without accountability. CEO compensation grew 1,094% from 1978 to 2024 while typical worker compensation grew 26%. Mancur Olson argued that collective action becomes more tractable — meaning identifiable and operationally approachable — when the target is symbolic and sufficiently concentrated. The SEC/Mercyhurst report's own data bears this out: 73% of activism-motivated incidents involved two or more individuals. Violent incidents were driven primarily by criminal motives and personal grievances, not activism — different populations requiring fundamentally different responses. Treating them as the same underlying trend is not analysis. It is storytelling in the language of analysis. That may serve a commercial purpose. It does not serve analytical integrity.

Three Disciplines, One Conflation: Symptom Response vs. Root Cause Analysis

Corporate security was built around a protective mandate. Protective intelligence represents a genuine advance — its proactive orientation, threat assessment methodology, and pre-incident indicator analysis are meaningful steps toward anticipatory security practice. But protective intelligence remains fundamentally investigative in its logic. It begins with a subject and works forward: who is this person, what is their history, what is their trajectory toward harm? Even at its most proactive, it asks a subject-centric question within a protective frame.

Intelligence and conflict analysis ask a structurally different question: what conditions are generating threats, and how are those conditions evolving? The unit of analysis is not the individual but the environment — the grievance landscape, the political economy, the distribution of institutional trust. Protective intelligence identifies individual actors earlier in the pathway to violence. It does not, by design or training, ask why the population of potential threat actors seems to be growing. That question requires a different discipline entirely.

This distinction has direct implications for prevention. Reactive detection — however sophisticated — is structurally incapable of comprehensive prevention. It will catch some actors. It will miss others. And it will do nothing to address the environment generating new actors. Intelligence analysis oriented toward structural conditions operates upstream of the pathway entirely. It does not ask who is approaching. It asks why the approach is becoming more likely. The overarching risk intelligence field is actively navigating this tension. The question is whether it resolves toward rigor or toward convenience.

The Programmatic Consequence: When Flawed Analysis Builds Surveillance Infrastructure

None of this is to suggest the underlying organizational concern is irrational. Low probability, high consequence events — an armed attack on a named executive, a kidnapping, a targeted assassination — represent exactly the kind of tail risk that justifies significant protective investment. The question is not whether to spend. The question is what the spend should be building. An organization that invests heavily in workforce surveillance on the basis of an undemonstrated causal chain is not managing tail risk. It is paying for the appearance of managing it while the actual threat profile goes underanalyzed. The spend may be rational. The shape of it is not.

The scale of the programmatic response is not hypothetical. According to Equilar's analysis of S&P 500 proxy statements, the share of companies providing security perquisites to executives rose 27.8% between 2023 and 2024 — from 24.5% to 31.3% — and a further 12.8% in 2025, with over a third of S&P 500 companies now providing security perks. Median executive security spending more than tripled from 3,068 in 2021 to 30,468 in 2025. Allied Universal, one of the largest security

services companies in North America, reported that requests for executive protection assessment and services increased 10 to 15 times following the December 2024 UnitedHealthcare CEO assassination. Yet Allied Universal's own president cautioned that the resulting proxy data is unreliable for benchmarking — driven by panic spending in the first 30 days, not calibrated risk assessment. Kevin Palacios, CEO of HELPS Latam and chair of the ASIS International Executive Protection Community, observed that many organizations responded by hiring visible security without addressing the actual problem — treating, in his words, a symptom, not the disease.

The SEC/Mercyhurst report documents that activism-motivated incidents — the largest single motive category — are overwhelmingly non-violent, rooted in specific political and economic grievances, and carried out by actors with no prior connection to the targeted executive. That profile does not describe an insider threat. The genuinely dangerous incidents — personal-motive attacks where nearly 80% of assailants are armed — warrant specific, targeted responses: threat assessment, pre-incident indicator analysis, residential security hardening, and travel risk management. What they do not warrant is the wholesale surveillance of workforces on the basis of a causal story the data does not tell.

Toward Strategic Risk Intelligence

The intelligence discipline has standards for a reason. Finished analysis is supposed to be distinguished from raw reporting. Alternative hypotheses are supposed to be considered and tested. Causal claims are supposed to be supported by evidence that goes beyond correlation and professional intuition. When those standards are relaxed — when the aesthetic of rigor substitutes for its substance — the consequences are not merely academic. They are organizational, ethical, and in some cases borne by people who had no say in the analysis that put them under scrutiny.

There is also a practical argument that does not require anyone to act in good faith. Reactive detection — however sophisticated, however well-resourced — is structurally incapable of comprehensive prevention. A program oriented toward identifying individuals who have already entered a pathway to harm will always be operating after the conditions that produced that pathway have taken hold. It will catch some actors. It will miss others. And it will do nothing to address the environment generating new actors. No amount of additional investment in detection changes this structural reality.

Strategic risk intelligence offers something reactive programs cannot: the possibility of intervening before the pathway forms. By engaging seriously with the structural conditions — the grievance landscape, the mobilization dynamics, the specific industries and executives whose risk profiles are genuinely elevated — an analytically grounded intelligence function can inform decisions that change those conditions. That is a capability argument, not a values argument. It does not require senior leaders to care about the employees being surveilled. It requires only that they prefer programs that work over programs that look like they work.

How is Strategic Risk Intelligence Operationalized?

The argument made in this paper points toward a different model of practice that is both achievable and demonstrably more effective — in terms of providing value across the enterprise — than the surveillance-heavy programs this paper critiques.

The core insight is organizational as much as analytical. The gap between protective intelligence and genuine strategic risk intelligence is not closed by hiring smarter analysts or deploying better technology. It is closed by building a team whose mandate, composition, and operating model are fundamentally distinct from anything the corporate security field currently recognizes as standard practice.

That team is interdisciplinary. It comprises analysts who are experts at becoming experts — professionals capable of rapidly developing deep contextual fluency across domains that most organizations treat as separate silos. It speaks the languages of every risk owner in the enterprise: the language of Geopolitical and Economic Strategy, of Legal, Compliance, and Regulatory risk, of Financial and Market Risk, of Information and Cyber Security, of Physical Security, Safety, and Resilience, and of ESG, Reputational, and Human Capital risk. Not just a superficial understanding, but with enough analytical depth to earn a seat at each table, synthesize across all of them, and surface the connections that no single domain owner can see from inside their own function.

This is the distinctive capability that strategic risk intelligence offers: cross-functional, mixed-method analysis that reveals root causes rather than cataloguing symptoms. It works upstream — not waiting for a threat actor to enter a pathway to harm, but analyzing the structural conditions that make that pathway more or less likely to be traveled. It partners with risk owners across the enterprise not to produce reports for filing but to drive decisions that build durable resilience. Its only mission is everyone else's sustainable success.

It is, in short, a team that breaks down silos by design — because the threats worth understanding most do not respect them.

The Integrated Risk Intelligence and Synthesis (IRIS) framework, developed by the author, provides a structured architecture for building and operationalizing this kind of function. IRIS translates the analytical principles argued for throughout this paper into a practical operating model: how the team is structured, how requirements are generated and prioritized across the six domains, how finished intelligence flows to decision-makers, and how the function integrates with — rather than displaces — existing protective intelligence and executive protection capabilities.

A fuller treatment of the IRIS framework, including its architecture, methodology, and implementation guidance, will be published separately. What this paper establishes is the analytical case for why such a framework is necessary.

About the Author

Jay Dunne is a senior global risk intelligence professional with 15 years of experience spanning GSOC leadership, strategic risk intelligence, protective intelligence, crisis management, and travel risk management in support of Fortune 500 companies. He most recently served as Manager of the Global Security Operations Center at Elevance Health. He holds an MS in Conflict Analysis and Resolution from George Mason University and a BA from Holy Cross College. He is the developer of the Integrated Risk Intelligence and Synthesis (IRIS) framework.

References

1. Security Executive Council and Mercyhurst University BI² Lab. Executive Targeting Report: Analysis of Attacks on Corporate Executives from 2003–2025. January 2026.

2. Economic Policy Institute. “CEO Pay in 2024.” September 2025. epi.org/publication/ceo-pay/

3. Economic Policy Institute. “The Productivity–Pay Gap.” August 2024.

4. Gurr, Ted Robert. Why Men Rebel. Princeton University Press, 1970.

5. Olson, Mancur. The Logic of Collective Action: Public Goods and the Theory of Groups. Harvard University Press, 1965.

6. Wilson, James Q., and George L. Kelling. “Broken Windows.” The Atlantic Monthly, March 1982.

7. Buil-Gil, David, et al. “Measuring the dark figure of crime in geographic areas.” British Journal of Criminology 61(2), 2021.

8. Equilar. “Executive Security Spending Shifts From Perk to Priority.” April 18, 2025. equilar.com/blogs/595-executive-security-spending-shifts.html

9. Equilar. “Executive Security Perks: Evolving Trends in a New Era of Risk.” Harvard Law School Forum on Corporate Governance, July 22, 2025.

10. Kucera, Glen. Quoted in Security Management. “Enterprise EP Spending Spiked in 2024, Still Right-Sizing After Targeted Attack.” ASIS International, April 30, 2025.

11. Meloy, J. Reid, and Jill Morikawa. “The Concept of Leakage in Threat Assessment.” Behavioral Sciences and the Law 18(4), 2000.

12. Calhoun, Frederick, and Steve Weston. Defusing the Risk to Judicial Officials. U.S. Department of Justice, 2003.

13. Hayes, Bob. “The Moment Workplace Incivility Became a Critical Threat Assessment Priority.” Security Info Watch, December 2025. securityinfowatch.com

14. Palacios, Kevin. Quoted in ASIS International Security Management. “How Executive Protection is Changing One Year After UnitedHealthcare CEO Attack.” December 4, 2025.

15. Allied Universal. 2025 World Security Report. October 2025.

16. “Incivility Is Becoming a Security Issue for CSOs.” Security Info Watch, December 17, 2025. securityinfowatch.com