The Intelligence Gap in Executive Protection

February 2026

Why Corporate Security Must Evolve to Prevent Harm

INSIDE

Executive Risk in a Changing Threat Landscape

By Peeler Group International

Targeted attacks against corporate leaders are increasing in frequency, complexity, and impact. As physical violence, insider escalation, and online radicalization converge, traditional security models built on alerts and reporting are no longer enough.

This special feature examines the evolution of executive threats, the behavioral patterns that precede violence, and why modern organizations must shift from information gathering to true protective intelligence. From pre-incident surveillance and evidence-based threat analysis to real-world operational prevention, this article outlines the critical capabilities shaping the future of executive protection.

Inside, we explore real case patterns, emerging risk drivers, and practical intelligence strategies designed to anticipate threats before harm occurs. →

The threat environment facing corporate executives has changed in ways that many organizations have not fully adjusted to. Recent research analyzing attacks on business leaders across more than two decades makes one reality clear: executive risk is rising, becoming more complex, and expanding beyond the traditional view of isolated criminal acts.

The Executive Targeting Report, released by the Security Executive Council, examined hundreds of real-world incidents involving corporate leaders worldwide. What stands out is not just the volume of attacks, but the acceleration in recent years. Physical assaults continue to dominate, while cyber-related and hybrid incidents are growing. CEOs remain the most visible targets, yet non CEO senior leaders are increasingly being targeted as well. This reflects a broader exposure of leadership teams rather than a narrow focus on one individual at the top. →

While these findings are concerning, the larger issue is how the private sector is responding to them.

Many corporations now collect massive amounts of threat-related information. They monitor social media, subscribe to alert platforms, track incidents globally, and generate daily or weekly reports. Yet collecting information is not the same as producing intelligence.

Information tells you something happened.
Intelligence explains why it happened, what it means, and what is likely to happen next.

That distinction matters.

True protective intelligence is not built on dashboards alone. It is built on analysis, behavioral understanding, and contextual interpretation. Without those elements, organizations are often left to react to events rather than anticipate and prevent them.

The Role of Behavior in Turning Information into Intelligence

One of the most overlooked components of modern threat assessment is human behavior. Violent acts targeting executives rarely emerge without warning signs. Decades of research across protective services, law enforcement, and behavioral science consistently show that individuals who commit targeted violence typically demonstrate observable changes and escalation patterns beforehand.

These behaviors often include:

- Fixation on a person, organization, or grievance
- Increasing emotional intensity or ideological rigidity
- Isolation and withdrawal from normal social circles
- Deception or secrecy surrounding movements or intentions
- Escalating language, threats, or hostile communication
- Rehearsal behaviors such as visiting locations, testing access, or seeking information

These are not theoretical concepts. They are evidence-based indicators that have been repeatedly identified in threat assessment studies and real-world attack investigations.

When corporate security programs rely solely on keyword monitoring, alerts, or volume of online chatter, they miss the patterns that actually signal risk. A single post may mean nothing. A consistent behavioral trajectory over weeks or months can mean everything.

This is where information becomes intelligence.

Behavioral analysis provides the context that allows analysts to distinguish between noise and credible threat development. It helps identify when frustration is turning into grievance, when grievance is turning into fixation, and when fixation is turning into preparation.

Pre-Surveillance Indicators: The Missed Warning Layer

Another critical area often absent from corporate protective programs is surveillance detection.

Targeted attacks, particularly those involving physical harm, frequently involve some form of pre-incident surveillance. Attackers commonly observe routines, study access points, test security responses, or revisit locations multiple times before acting.

Documented pre-surveillance indicators include:

- Repeated presence in areas tied to an executive's routine
- Individuals photographing entrances, vehicles, or security features
- Unusual questions about schedules, access, or movements
- Vehicles lingering or returning in consistent patterns
- Attempts to blend into environments without a legitimate purpose

These behaviors have been identified across military, law enforcement, and executive protection operations for decades. Yet in the corporate environment, surveillance detection is often treated as a specialty skill rather than a foundational protective measure.

In many organizations, surveillance detection remains confined to specialized teams or theoretical training rather than being embedded into daily facility security operations. Frontline personnel are rarely trained to recognize pre-incident indicators, document behaviors objectively, or escalate patterns for analysis. This disconnect leaves a critical prevention layer unused at the very point where early warning signs most often appear.

Without surveillance detection built into daily operations, organizations are blind to the preparation phase of attacks.

Protective intelligence should not exist only in reports. It must be connected directly to executive protection teams, facility security, and frontline personnel who are trained to recognize and report these indicators in real time.

This is where intelligence moves from abstract analysis into operational prevention.

Evidence-Based Behavioral Reporting Matters

Another gap in many private sector programs is how behavior is documented.

Too often, reports rely on vague descriptions such as:

“Suspicious individual observed.”
“Concerning online activity noted.”
“Possible threat identified.”

These statements are subjective and difficult to analyze.

Evidence-based reporting focuses on observable facts:

- What was said or done
- How frequently it occurred
- Where it occurred
- Changes over time

Specific actions taken

For example, “individual appeared angry” is not intelligence.
“An individual sent five messages over three days expressing grievance and referencing the executive by name” is intelligence.

This style of reporting allows analysts to identify escalation trends, correlate behaviors across sources, and assess risk with greater accuracy.

It also creates defensible documentation that supports interventions, law enforcement coordination, and protective decisions.

> Behavior that is tracked objectively becomes measurable.
> Measurable behavior becomes analyzable.
> Analyzable behavior becomes actionable intelligence.

A Call to Lead — Not Just Manage Security

The Executive Targeting Report is not a call to fear – it’s a strategic warning. The world we operate in now is more open, more connected, and more volatile. Attackers are not monolithic. They are influenced by ideology, grievance, opportunity, and sometimes by nothing more than viral narratives.

Corporate security leaders should take these insights not as another risk metric, but as a mandate to evolve:

→ Demand intelligence frameworks that include behavioral insight.
→ Invest in cross-disciplinary analytic capability.
→ Integrate psychology and social science understanding into threat modeling.
→ Shift from reactive event management to predictive threat anticipation.

Because prevention isn’t an outcome → it’s a capability.

Intelligence Must Move from Abstract to Real World Action

One of the most common failures of corporate intelligence programs is that insight never fully translates into operational change.

Threat reports are produced.
Risk levels are assigned.
But executive movement planning, security posture, and mitigation strategies often remain unchanged.

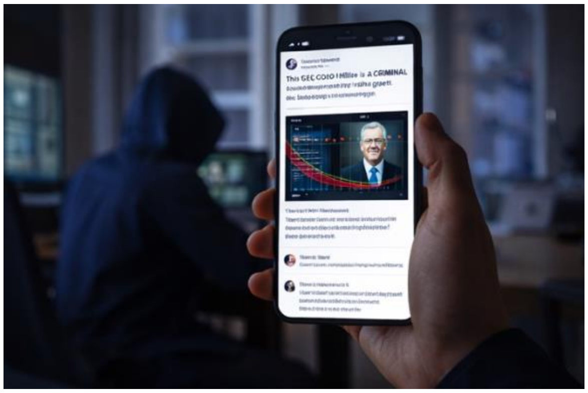
But executive movement planning, security posture, and mitigation strategies often remain unchanged.

Intelligence without action is simply information.

Protective intelligence should drive:

- Adjustments in travel routes and schedules
- Increased surveillance or monitoring where risk rises
- Executive protection posture changes
- Facility security enhancements
- Early engagement with law enforcement or threat teams
- Direct mitigation of emerging threats

When intelligence is embedded into daily operations, it stops being a theoretical exercise and becomes a living protective system.



The Missing Drivers of Modern Executive Risk Narrative Radicalization and the Online to Real World Pipeline

Today’s threat actors are increasingly influenced by online narratives rather than isolated personal grievances alone.

Social platforms amplify outrage.
Echo chambers reinforce perceived injustice.
Disinformation fuels hostility.
Group validation normalizes violent rhetoric. →

Many attackers now progress through a pathway of:

- Online grievance building
- Fixation on a person or company
- Public validation of anger
- Rehearsal behaviors
- Real-world action

Leakage: When Intent Is Signaled Before Violence

Another well-documented phenomenon in targeted violence research is leakage.

Most attackers communicate their intent in some form before acting. This may include:

- Threatening statements
- Online posts expressing revenge or justice
- Sharing violent ideation
- Telling acquaintances about plans
- Posting manifestos or symbolic messages

These signals are often dismissed as venting or exaggeration.

In reality, they are among the most reliable pre-incident indicators.

Without behavioral interpretation and evidence-based documentation, these warning signs are frequently overlooked until after violence occurs.

Alert Fatigue and the Danger of Treating Everything as High Risk

Many corporate programs generate enormous volumes of alerts.

When every signal is treated as urgent:

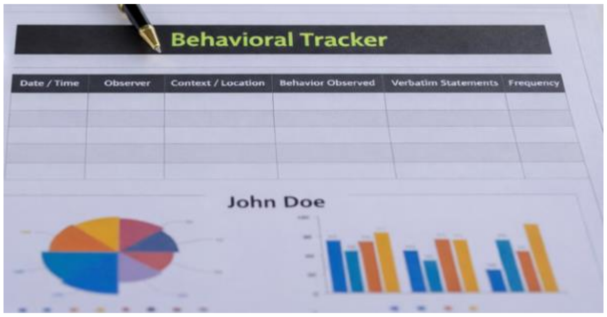
- Analysts become overwhelmed
- Prioritization breaks down
- Decision makers disengage
- Real threats blend into noise

Protective intelligence is not about flagging everything.

It is about identifying credible escalation trajectories among thousands of data points.

Behavioral analysis enables organizations to focus resources where risk is actually developing.

Insider Threat and Proximity Risk



While many attackers are strangers, a significant portion of serious incidents involve individuals with prior access or familiarity.

These may include:

- former employees
- customers
- Contractors’
- business partners
- disgruntled insiders
- individuals with routine exposure to facilities or schedules

→ Proximity increases both opportunity and lethality.

→ Behavioral changes within organizations are often among the earliest warning signs of escalation.

→ Ignoring insider behavioral risk leaves a critical blind spot in protective intelligence programs.

Leadership Culture and Decision Support

THREAT ASSESSMENT
Escalating Risk Level 1.32
HIGH
Online Threats Targeting Executive
Suspicious Activity in Vicinity
Surveillance Indications
Behavioral Escalation

Even the strongest intelligence programs fail without executive understanding and engagement.

When intelligence is:

- Too technical
- Too abstract
- Poorly translated into business risk
- Not tied to real consequences

Protective action stalls.

High-performing programs present intelligence in clear, actionable terms that directly support leadership decisions on movement, operations, and risk tolerance.

Measuring Prevention, Not Just Incidents

Traditional metrics focus on what happened after harm occurred.

Advanced intelligence programs measure:

→ Escalation patterns detected early
→ Surveillance attempts identified
→ Behavioral threats mitigated
→ Interventions conducted
→ Protective adjustments made proactively

These metrics reflect prevention, not reaction.

The Critical Role of Meaningful Executive Communication

One of the most underestimated risk factors in executive protection is the relationship between security professionals and the principals they protect.

Executives often shape their own security posture based on:

- → Convenience
- → visibility concerns
- → perceived normalcy
- → personal comfort
- → assumptions about risk

Without ongoing, meaningful communication grounded in real threat assessment, principals may unknowingly undermine protective measures.

When leaders self-direct security rather than rely on professional analysis, protection becomes fragmented and inconsistent.

True protective intelligence must include continuous dialogue with executives that explains:

- → evolving threat environments
- → behavioral risk indicators
- → why specific protective measures are needed
- → how intelligence translates into safety

When leaders understand risk in real terms, compliance increases, and protection becomes effective.

Where Corporate Security Continues to Fall Short

Across industries, consistent gaps remain:

- > Overreliance on technology without human analysis
- > Limited behavioral expertise in intelligence teams
- > Minimal surveillance detection integration
- > Subjective reporting practices
- > Alert saturation without prioritization
- > Weak translation from intelligence to action
- > Insufficient executive engagement
- > Breakdowns in meaningful communication with principals, leading executives to self-navigate security decisions rather than follow assessment-driven protective strategies

These gaps allow threats to mature unnoticed.

Intelligence Is About Understanding People and Preventing Harm

Data alone will never stop violence.

Understanding behavior, escalation, preparation, and intent enables organizations to intervene before harm occurs.

Protective intelligence that incorporates behavioral evidence, surveillance detection, narrative analysis, and real-world operational response transforms security from reactive to preventive.

If corporate security is to meet today's threat reality, it must move beyond information collection.

It must build intelligence systems that understand people, identify risk early, communicate effectively with leadership, and act decisively in the real world.

Critically, protecting senior leadership is not solely an operational or security function. BOD level awareness, input, and decision-making are essential components of corporate diligence in safeguarding people within the organization. When leadership protection is treated as a governance responsibility rather than a discretionary service, alignment improves, resources follow risk, and prevention becomes achievable.

→ That is how information becomes intelligence.
→ That is how intelligence becomes protection.
→ And that is how prevention becomes possible.

A Personal Perspective from the Field

Over the course of my career across law enforcement, investigations, executive protection, and corporate security, I have seen threat landscapes evolve while one reality remains constant: targeted violence rarely occurs without warning, and prevention is possible when intelligence is properly understood and operationalized.

In recent years, intelligence has become a corporate selling point. Dashboards, monitoring platforms, and reports are often labeled as intelligence, yet many still reflect information rather than true analysis of escalation, intent, and required action. More concerning is what frequently fails to reach those protecting executives in the field. Actionable intelligence that informs movement planning, posture adjustments, and mitigation is often absent, leaving protective teams without the behavioral context needed to prevent harm.

I have also observed organizations reducing physical protective measures under the assumption that intelligence monitoring alone is sufficient. Intelligence and physical protection were never meant to replace one another. Protective intelligence should guide where and how resources are deployed through a risk-established approach that integrates behavioral analysis, surveillance detection, operational protection, and executive movement planning into a unified prevention strategy.

Equally important is executive decision-making. Leaders should not be their own security advisors. When risk is clearly communicated through real-world indicators and escalation patterns, protective measures can be implemented in ways that preserve productivity and lifestyle while quietly reducing exposure.

True protective intelligence is not about fear. It is about foresight. When intelligence informs operations and leadership decisions in real terms, prevention becomes achievable.

Bill Peeler

– Bill Peeler, Founder, Peeler Group International

Appendix A

Key Terms and Concepts in Protective Intelligence

Protective Intelligence

The integration of behavioral analysis, threat assessment, surveillance detection, and operational response is designed to identify escalation pathways and prevent targeted violence before harm occurs.

Behavioral Escalation Trajectory

The observable progression through which individuals move from grievance to fixation, preparation, and action. This includes emotional hardening, hostile communication, isolation, rehearsal behaviors, and intent signaling.

Pre-Incident Surveillance Indicators

Actions commonly used by attackers to assess routines, access points, and security posture before an incident. These may include repeated presence, photography, schedule probing, unusual questioning, and pattern observation.

Leakage

The communication of intent prior to violence through statements, online posts, symbolic actions, or conversations with others. Leakage is one of the most consistent pre-incident indicators in targeted violence research.

Narrative Radicalization

The process by which individuals become emotionally and ideologically reinforced through online or group environments that amplify grievance, normalize hostility, and justify violent action.

Evidence-Based Behavioral Reporting

Objective documentation of observable actions, including frequency, escalation, location, and specific behaviors, rather than subjective impressions. This reporting enables pattern recognition and defensible risk assessment.

Risk-Established Deployment

The allocation of protective resources based on evolving threat trajectories and behavioral indicators rather than static security models or convenience-based protection.

Surveillance Detection Integration

Embedding pre-incident behavior recognition into frontline security operations, executive protection teams, and facility personnel as a core prevention capability.

Actionable Intelligence

Analyzed information that directly informs operational decisions such as movement planning, posture adjustments, mitigation strategies, and early intervention.

Governance-Level Protection Oversight

The involvement of executive leadership and Boards of Directors in risk awareness, protective strategy alignment, and duty-of-care accountability for leadership safety.

Appendix B

Practical Protective Intelligence Integration Framework

This framework illustrates how organizations translate behavioral indicators into real-world prevention.

Early Behavioral Detection

- Grievance expression online or internally
- Escalating hostile language
- Fixation on leadership or organization
- Emotional hardening and isolation
- Rehearsal behaviors or probing activity

Output: Escalation trajectory identified

Evidence-Based Documentation

- Objective behavioral descriptions
- Frequency and pattern tracking
- Correlation across platforms and locations
- Timeline development
- Behavioral severity assessment

Output: Defensible intelligence profile

Surveillance and Preparation Recognition

- Repeated presence near executive routines
- Photography or mapping activity
- Schedule probing
- Access testing
- Patterned observation

Output: Transition from grievance to preparation confirmed

Intelligence-Driven Operational Response

- Adjust executive movement routes and timing
- Increase protective posture where risk escalates
- Enhance monitoring of the threat subject
- Modify facility access controls
- Engage threat management or law enforcement

Output: Risk mitigated before harm occurs

Executive Communication and Governance Alignment

- Clear explanation of behavioral risk trajectory
- Operational impacts communicated in real terms
- Protection strategy aligned with leadership tolerance
- Governance oversight applied where required

Output: Prevention supported and sustained

Prevention-Focused Performance Indicators

Rather than measuring harm after it occurs, mature programs track:

- Escalation patterns identified early
- Surveillance attempts detected
- Behavioral threats mitigated
- Interventions conducted
- Protective adjustments made proactively

These metrics reflect the effectiveness of prevention.

Integrated Outcome

When behavioral analysis, surveillance detection, intelligence translation, operational protection, and leadership engagement function together, organizations move from reacting to incidents to preventing them.

This is the operational reality of true protective intelligence.

Is Your Organization Practicing Protective Intelligence?

- *Do you track behavioral escalation over time rather than isolated incidents?*
- *Are surveillance indicators actively embedded into facility and frontline security operations?*
- *Does intelligence consistently drive changes in protection posture and deployment?*
- *Are executives briefed in clear, real-world risk terms rather than abstract reports?*
- *Does the Board of Directors provide oversight and strategic direction for leadership protection?*

Organizations answering “no” to most of these questions are likely collecting information rather than practicing true protective intelligence.

WHO WE ARE - PEELER GROUP INTERNATIONAL

PGI PEELER GROUP INTERNATIONAL

Peeler Group International (PGI) is a globally positioned, mission-driven security, risk management, and investigative firm established in 1995. For nearly four decades, PGI has delivered tailored solutions that safeguard people, assets, and organizational resilience for both corporate and individual clients. The firm's work spans executive protection, comprehensive risk assessment, threat mitigation, crisis planning, and advanced investigative services – all grounded in real-world experience, operational excellence, and behavioral insight.

At the core of PGI's philosophy is a commitment to protective intelligence that integrates analysis with action, ensuring that risk is not only identified but prevented. From Fortune-level executive protection programs to bespoke security strategies for high-profile individuals, PGI blends situational understanding, observable behavioral analysis, and tailored operational planning to deliver meaningful, measurable security outcomes.

Founded by security professionals with decades of frontline experience, PGI's approach emphasizes actionable insight over abstract reporting, prioritizing early recognition of risk and precise deployment of protective resources. With licensed operations across multiple U.S. jurisdictions and a global operational footprint, PGI serves organizations navigating complex threat environments where leadership exposure, reputation, and continuity are critical.

Beyond operational services, PGI advises boards, executives, and security leaders on building intelligence-driven protection programs that translate risk into informed decision-making. Through executive briefings, strategic consulting, and speaking engagements, PGI helps organizations move from awareness to prevention by aligning leadership, intelligence, and action.

For inquiries regarding executive briefings, advisory services, or speaking engagements,
visit **peelergroup.com** or email **info@peeler-group.com**

Supporting Your Success, Safety and Security