— BRIEFING / 033 · SEPTEMBER 2026

THE ESCALATION CURVE

A case unfolding in New York this summer traces, with textbook clarity, the trajectory grievance-driven targeting of executives almost always follows. We publish it without names, because the names are not the lesson. The curve is.

EXECUTIVE RISK SERVICES

Prepared for worst-case scenarios. So you don't have to.

info@executiveriskservices.com · referral or invite only

— 01 / THE CASE, AT THE ALTITUDE THAT MATTERS

THE CASE, AT THE ALTITUDE THAT MATTERS

A senior executive at a prominent New York company spent months as the subject of escalating threats posted online, explicit enough to include threats against her life. This summer, the person behind those posts appeared in person at the company's headquarters. He remains at large, and the matter is with law enforcement. Every identifying detail beyond that is deliberately omitted here: this briefing exists because the sequence is common, not because the case is unusual.

— 02 / THE BACKDROP DATA

THE BACKDROP DATA

Research on targeted violence against corporate leaders gives the case its context. Security Executive Council analysis of executive-targeting incidents spanning two decades finds the volume climbing sharply, with 2025 running at roughly double 2024. Roughly three quarters of perpetrators are strangers to their targets, and while activism motivates the largest share of incidents overall, the violent subset is driven disproportionately by personal grievance, a perceived injury the target usually knows nothing about. The stranger statistic is the one that should reorganize programs, because every traditional insider-focused instrument, HR files, exit interviews, workplace reporting channels, is blind to it.

— 03 / THE CURVE

THE CURVE

Grievance-driven targeting rarely begins at the door. The documented pathway runs through observable stages. A grievance attaches to a person rather than an institution, and fixation narrows: one name appears more often, then constantly. Language shifts from anger about to intention toward, from insult to ultimatum. Research and rehearsal behaviors follow, often visible in what the subject posts, asks, or seeks. And then comes the boundary probe, the first physical presence, an approach, a visit, an appearance at a place associated with the target, testing whether the distance between saying and doing still holds. Each stage is observable. Each is more expensive to interrupt than the one before it. The New York case reached the boundary probe with, by all public indications, no protective structure watching the earlier stages.

— 04 / THE DISCIPLINE THAT CATCHES IT

THE DISCIPLINE THAT CATCHES IT

The instrument built for this curve is protective intelligence, and its logic differs from both cybersecurity and guarding. It monitors open sources for fixation on named principals, not for keywords but for trajectory: frequency, narrowing, language shift, leakage of intent. It assesses patterns rather than adjudicating individual posts, because the curve lives between messages, not inside any one of them. It maintains the connective tissue that most programs lack, a live channel between assessment and physical security, so that the lobby, the reception desk, and the detail know the face and the vehicle before either arrives. And it treats law enforcement engagement as a managed relationship with thresholds decided in advance, not a decision improvised on the day the subject appears.

— 05 / THE READ

THE READ

Most organizations still budget online threat monitoring and building security as separate lines that meet only after an incident. The escalation curve does not respect that boundary, and the year's data says the curve is being walked more often. The question a board should ask its security leadership is specific: if fixation on one of our executives were building online today, at what stage would we first know, and who would tell the front door. If the honest answer is the boundary probe, the program is set to learn about its threats in person.

— 06 / SOURCES AND METHOD

SOURCES AND METHOD

This briefing draws on August 2026 reporting of a New York case, deliberately de-identified, and on published Security Executive Council executive-targeting research. We characterize threat content without quoting it, name no individuals, and speculate on no ongoing investigation. The pattern is public property; the people in it are not.