OIQ Executive Threat Matrix (2025)

The risks executives face are no longer confined to boardrooms or secure compounds. They emerge from digital exposure, escalate through online chatter, and manifest as physical danger.

This Threat Matrix maps the ten most pressing categories of executive risk in 2025. Each is scored on a **1–10 scale for risk and severity**.

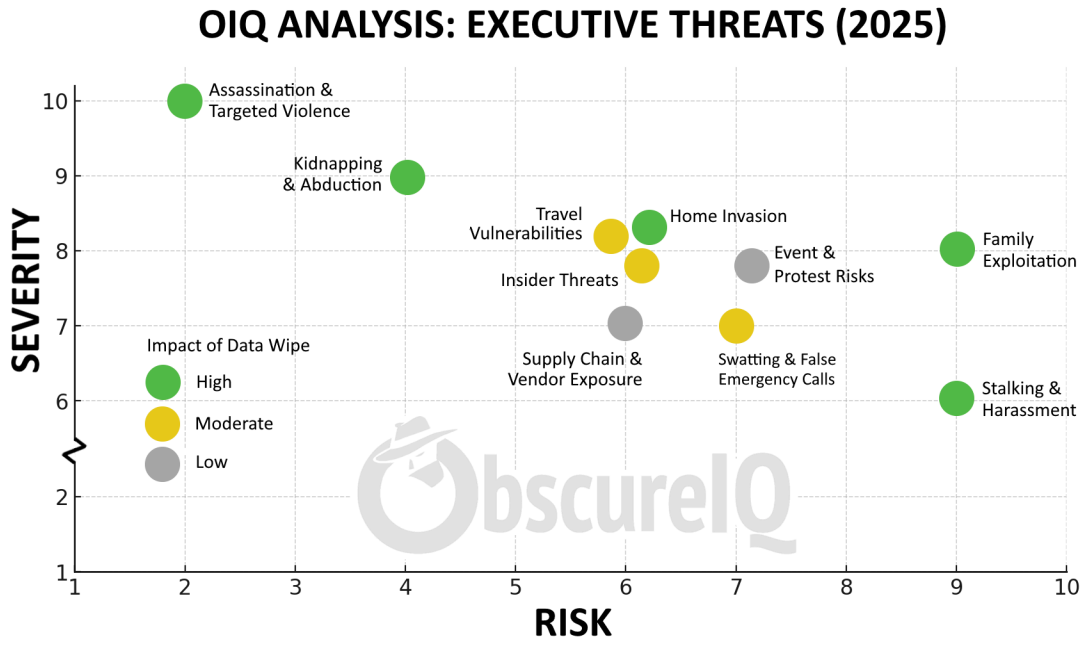
- **Risk**: How often the threat occurs or is attempted.
- **Severity**: The potential impact if realized.

The goal is not alarmism. It is clarity. Executives are targeted in predictable ways, and each pathway begins with **digital breadcrumbs**. Exposed addresses, leaked credentials, family social posts.

This document highlights:

- The **threat categories** most relevant to Fortune 500 leaders and high-visibility figures.
- The **digital triggers** adversaries exploit to escalate from data to danger.
- The **patterns of adversary behavior** seen across recent cases.
- The **counter-moves** that close exposure before it becomes exploitation.

Control the footprint. Control the threat.



Comparing Threats Against Executives (2025)

Threat Category	Risk	Severity	Digital Triggers	Risk Reduction Potential
Assassination & Targeted Violence	2	10	Home addresses, travel itineraries, extremist chatter	High – Suppressing addresses and itineraries removes the most common targeting vectors.
Home Invasion	6	8	Property records, vacation home leaks, contractor data	High – Broker suppression and property data control directly lower attack surface.
Kidnapping & Abduction	4	9	Family posts, school listings, travel routines	High – Family footprint erasure + education closes the most common planning vectors.
Stalking & Harassment	9	6	Doxxing, leaked numbers, obsessive online attention	High – Rapid doxxing suppression and takedowns directly cut harassment channels.
Swatting & False Emergency Calls	7	7	Residential addresses, spoofed caller IDs	Medium – Wiping addresses reduces opportunities, but spoofed IDs are harder to control.
Travel Vulnerabilities	6	8	Flight tracking, LinkedIn updates, conference schedules	Medium – Travel info leaks often come from public disclosures, not just brokers.
Family Exploitation	9	8	Social posts, Venmo transactions, relative exposure	High – Family-focused suppression and monitoring are critical to reducing this risk.
Event & Protest Risks	7	8	Event announcements, activist forum chatter	Low–Medium – Wiping helps with itinerary leaks, but events are public by design.
Insider Threats	6	8	Leaked credentials, online grievances, LinkedIn exposure	Medium – Digital suppression helps, but insider intent is a separate variable.
Supply Chain & Vendor Exposure	6	7	Contractor profiles, invoices, vendor oversharing	Low–Medium – Vendor behavior often outside the exec's control; limited reduction.

1. Assassination & Targeted Violence

Risk: Low, but catastrophic when it occurs.

Why it matters:
Executives tend to dismiss assassination risk as remote. They're not heads of state, after all. But recent cases prove that the line between online hate and physical action has thinned. In an era where social media mobilizes strangers and AI deepens grievances, targeted violence can escalate from rhetoric to reality faster than traditional security teams can react.

Digital Triggers:

- Data broker sites publishing home addresses and property records.
- Conference agendas and LinkedIn posts pinpointing time and place.
- Online chatter in fringe forums, often dismissed until after the attack.

Adversary Behavior:
Attackers don't need inside help anymore. They stitch together open-source fragments: an exposed address here, a leaked flight detail there. This forms a digital "attack map" that guides timing and location.

Counter-Moves:

- **Suppress**: Remove home addresses, property filings, and related family data from people-search and broker sites.
- **Monitor**: Track open, deep, and dark web chatter for escalations targeting the principal.
- **Compartmentalize**: Obscure travel patterns, limit agenda disclosures, and compartmentalize comms so itineraries can't be pieced together.

If your home address is still on a data broker site, your security detail is already playing catch-up.

2. Home Invasion

Risk: Medium. Increasing with digital exposure.

Why it matters:
Corporate offices are hardened. Residences are not. Executives often own multiple homes — a penthouse, a vacation property, a rural retreat. Each new address expands the attack surface. For adversaries, a softer perimeter makes the residence the easiest place to strike.

Digital Triggers:

- Property records exposed on people-search sites.
- Real estate listings and satellite images confirming layouts.
- Family posts geotagging secondary residences.
- Utility contractors or service vendors leaking client details.

Adversary Behavior:
Criminals no longer need to follow an executive home. They can map entry points and confirm occupancy through digital leaks. Vacation properties are particularly vulnerable — empty for months, low surveillance, easy targets.

Counter-Moves:

- **Suppress**: Remove property addresses from brokers and real estate archives.
- **Audit**: Review secondary and vacation homes with the same rigor as primary residences.
- **Deceive**: Obscure occupancy patterns — lights, utilities, travel disclosures — to deny adversaries an easy window.

If your vacation home is listed on a data broker site, it's not a getaway — it's a soft target.

3. Kidnapping & Abduction

Risk: Rare domestically, higher abroad.

Why it matters:
Kidnapping is a low-frequency, high-severity risk. While uncommon in the U.S., executives traveling internationally — or their families at home — face real exposure. Kidnappers are motivated by ransom, revenge, or politics. Their planning is increasingly digital.

Digital Triggers:

- Children's Instagram or TikTok posts revealing school, routines, or vacations.
- School addresses indexed on people-search sites.
- Travel announcements in press releases or family social posts.

Adversary Behavior:
Target selection starts with perceived vulnerability. Family members are often the softest flank. Attackers harvest digital signals to time abductions — a child's soccer schedule, a spouse's flight delay, or a vacation post that confirms no one is home.

Counter-Moves:

- **Erase**: Suppress family records, especially minors' school or extracurricular details.

- **Educate**: Train family members to recognize what not to post.
- **Protect**: Deploy covert travel protocols and vetted transportation for international trips.

If your child's school appears in a Google search, the adversary has already found their window.

4. Stalking & Harassment

Risk: High. Often the precursor to worse.

Why it matters:
Before an attack, there's obsession. Stalkers and harassers test boundaries digitally long before they escalate in person. This category is less about single catastrophic events and more about chronic exposure that erodes safety, sanity, and reputation.

Digital Triggers:

- Leaked personal phone numbers and emails.
- Social media oversharing by executives or family.
- Doxxing events where private details are published online.

Adversary Behavior:
Harassers thrive on access. Each contact detail is another way to intrude — calls, texts, DMs, doorstep visits. For many, the act of harassment is the attack itself. For others, it's rehearsal for something physical.

Counter-Moves:

- **Monitor**: Continuous sweeps for doxxing incidents, leaked numbers, and impersonation attempts.
- **Takedown**: Rapid suppression of personal data before it spreads.
- **Redirect**: Controlled communication channels to contain harassers and cut escalation paths.

Every doxxing event is a rehearsal. Ignore it, and you invite the encore.

5. Swatting & False Emergency Calls

Risk: Rising sharply.

Why it matters:
Swatting has moved from internet pranks to targeted attacks on executives, judges, and

politicians. A false 911 call can weaponize local police, bringing armed responders to an executive's front door. Even when no one is harmed, the trauma, reputational fallout, and security strain are real.

Digital Triggers:

- Home addresses exposed on data broker sites.
- Spoofed phone numbers from breach dumps.
- Publicized names tied to residential locations.

Adversary Behavior:
Attackers use exposed addresses and hacked or spoofed caller IDs to stage convincing emergencies. Law enforcement, acting in good faith, becomes the vector of attack. Executives with multiple residences are particularly vulnerable — each property is another address to weaponize.

Counter-Moves:

- **Pre-Brief**: Work with local police so your address is flagged against false reports.
- **Suppress**: Remove residential addresses from data brokers to reduce targeting opportunities.
- **Protocol**: Establish a family plan for emergency responses — who answers the door, who contacts legal, who notifies security.

If police know your address before the attacker calls it in, swatting fails before it starts.

6. Travel Vulnerabilities

Risk: Medium.

Why it matters:
Executives are most exposed when in transit. Airports, hotels, conference centers — unfamiliar environments with thin perimeters. Travel itineraries are often easier to find than executives realize, and attackers exploit predictable routines.

Digital Triggers:

- Flight data, sometimes scraped from public tracking services.
- Conference agendas and speaking slots posted online.
- LinkedIn updates or selfies that confirm locations in real time.

Adversary Behavior:
Adversaries look for gaps in the schedule. A flight delay means hours in an unsecured lounge. A

conference agenda pinpoints when the executive will be onstage. Attackers don't need to follow — digital breadcrumbs guide them.

Counter-Moves:

- **Compartmentalize**: Separate personal and professional travel channels to reduce data leakage.
- **Delay**: Post travel details only after departure, never live.
- **Cover**: Use controlled comms and burner devices abroad to limit metadata exposure.

If your LinkedIn reveals your conference schedule, it's not networking — it's targeting intelligence.

7. Family Exploitation

Risk: High.

Why it matters:
The family is the open flank. Children, spouses, and relatives have digital footprints of their own — often unprotected, often overlooked. Threat actors know that a family member's exposed data is as valuable as the executive's own.

Digital Triggers:

- Venmo or CashApp transactions exposing real-time locations.
- Instagram or TikTok stories showing daily routines.
- People-search records listing relatives and addresses.

Adversary Behavior:
When the principal is hardened, attackers pivot to the family. They monitor children's social media, track spouses' travel, or exploit in-laws' addresses. The family becomes the pathway into the executive's life.

Counter-Moves:

- **Audit**: Extend footprint scans beyond the principal to the entire family circle.
- **Train**: Teach family members what not to post, what to lock down, and why.
- **Shield**: Monitor continuously for family-targeted doxxing or exposure.

Your executive protection plan fails the moment a child's TikTok gives away the home address.

8. Event & Protest Risks

Risk: Medium-High.

Why it matters:
Shareholder meetings, earnings calls, industry conferences — executives can't avoid the spotlight. But public events are magnets for activists, protesters, and opportunistic attackers. One breach at an event can bypass years of careful security.

Digital Triggers:

- Publicized event locations and times.
- Activist chatter on forums or Telegram channels.
- Travel leaks confirming the executive's presence.

Adversary Behavior:
Attackers don't guess. They monitor online discussions, coordinate protests, and use digital signals to predict exactly where and when executives will appear. Event disruption is often staged online weeks in advance.

Counter-Moves:

- **Sweep**: Conduct pre-event monitoring of social platforms, dark web chatter, and activist forums.
- **Blend**: Compartmentalize itineraries and control disclosures to limit public targeting.
- **Respond**: Train event staff in rapid threat response tied directly to digital intelligence feeds.

Every protest begins online. If you're not watching the chatter, you're walking blind into the crowd.

9. Insider Threats

Risk: Persistent, hard to detect.

Why it matters:
Executives are surrounded by employees, contractors, and consultants who have access to routines, spaces, and systems. Most are loyal. Some are not. A disgruntled insider doesn't need to hack in — they already know the passwords, the layouts, the shortcuts.

Digital Triggers:

- Leaked employee credentials on the dark web.

- Online rants from current or former staff.
- LinkedIn posts exposing roles, responsibilities, and access points.

Adversary Behavior:
Insiders exploit trust. They combine their knowledge with digital exposure — a leaked credential, a shared floorplan — to bypass barriers that outsiders struggle to cross. Many act after termination, when anger runs hot and access hasn't been fully revoked.

Counter-Moves:

- **Monitor**: Track leaked employee credentials and insider chatter online.
- **Audit**: Enforce rapid offboarding and least-privilege access.
- **Probe**: Run red-team scenarios that assume an insider is already inside.

If you don't know which ex-employee's password is for sale on the dark web, you're betting your safety on luck.

10. Supply Chain & Vendor Exposure

Risk: Rising, underestimated.

Why it matters:
Executives don't just depend on corporate staff — they rely on drivers, contractors, household staff, medical providers, and third-party vendors. Each is an entry point. A weak link in the supply chain can expose access to homes, offices, or even medical records.

Digital Triggers:

- Contractors listing executive clients on their websites or LinkedIn profiles.
- Vendor invoices that leak addresses or schedules.
- Medical or wellness staff posting about "celebrity clients."

Adversary Behavior:
Attackers target the overlooked layer. Instead of going at the armored SUV, they approach the driver at his side job. Instead of hacking the CISO, they breach a vendor with weaker defenses. For adversaries, the chain is only as strong as its weakest subcontractor.

Counter-Moves:

- **Vet**: Audit vendors for digital hygiene and confidentiality.
- **Restrict**: Limit how contractors handle or publish information tied to the executive.
- **Monitor**: Extend digital sweeps to include vendors who have proximity to the principal.

Your driver's LinkedIn can compromise you faster than your own.

We Protect the Critical Few.

Uncompromising privacy and intelligence services for people with everything to lose.

Digital Executive Protection | Risk Audits | Privacy Recovery | Threat Mitigation