ironwall
by Incogni

Executive protection whitepaper

The hidden gap in executive protection

Why every protection program now requires a digital bodyguard

Who this is for

This whitepaper is intended for corporate security leaders, executive protection teams, and risk decision-makers responsible for safeguarding senior leadership in today's digital-first risk environment.

Summary

Executive protection usually focuses on what happens in the physical world: trained bodyguards, secure transportation, and well-defined emergency response protocols. Together, these measures form the foundation of traditional protection services.

But, because the internet has fundamentally changed the environment in which threats emerge, another layer of protection has become essential—a digital layer.

Threats against executives often take shape online long before they become tangible in the physical world. They start with a Google search. An individual seeking to harm someone—especially a relatively public figure like a CEO—can easily find their home address, contact details, family connections, routines, past locations, properties, and even floor plans of their home.

This creates a critical gap in many executive protection programs. Which is where the concept of a digital bodyguard comes into play.

Just as a physical bodyguard manages proximity, screens individuals, and secures environments, a digital bodyguard manages discoverability, screens potential threats, and secures personal information. It isn't a replacement for physical protection. It is its natural counterpart.

These two layers can work together to provide more comprehensive executive protection:

- Physical protection safeguards executives in the real world
- Digital protection limits exposure and prevents threats from escalating into physical attacks.

This whitepaper explores why executives are uniquely targeted, how digital exposure escalates into real-world danger, and how integrating a digital bodyguard into executive protection programs closes one of today's most dangerous security gaps.

Executives are high-risk targets

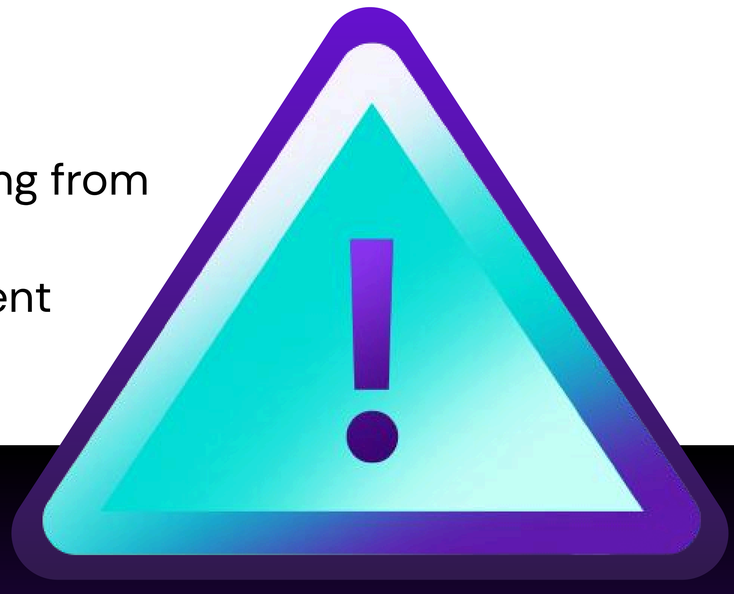
Executives occupy a unique position that makes them both more likely to be targeted by malicious actors and easier to reach. This is due to their visibility, influence, and perceived access to resources.

Unlike most employees, who can enjoy relative anonymity, executives are often associated with corporate decisions—from controversial policies and layoffs to pricing changes and public stances on social and political issues. This kind of public association can quickly turn business outcomes into perceived personal grievances. Often on a mass scale, and sometimes with serious consequences.

This is exactly what happened with the killing of UnitedHealthcare CEO Brian Thompson. And public hostility has only escalated since then, with US Homeland Security Secretary Alejandro Mayorkas stating, “It speaks of what is really bubbling here in this country, and unfortunately we see that manifested in violence, the domestic violent extremism that exists,”.[1]

The risks

Executives can, and do, face a wide spectrum of threats, ranging from harassment and intimidation to direct physical violence. The motivations may vary, but the enabling factor remains consistent across categories: access to personal information.



Physical

↑

Digital

Physical approach or attack
Trespassing, confrontation, assault, or targeted violence.

Stalking & surveillance
Attempts to track movements, routines, or physical locations.

Direct threats online
Messages, emails, posts, or calls referencing harm, intimidation, or demands.

Online targeting & hostile attention
Angry posts, harassment, fixation, doxxing, or coordinated hostility emerge.

Public data exposure
Personal details, locations, family info, habits, or affiliations are available online and sold by data brokers.

Organized hate and ideological targeting

Following the murder of Brian Thompson, the New York Police Department reported that social media posts circulated “wanted” posters and hit-list style imagery featuring the names and salaries of industry leaders.2 The goal was clear: to incite public outrage and targeted hate campaigns.
In such polarized online environments, names, photos, and personal details—all easily found online—become weapons that enable:

- Harassment of family members
- Targeting of personal social media accounts
- Creation of intimidation campaigns

Doxxing

Doxxing involves the public release of private or semi-private information with the intent to intimidate, shame, or encourage harassment. It's a method often used to punish or pressure public figures.

It happened to the former CEO of Turing Pharmaceuticals, Martin Shkreli, back in 2015, following controversial drug pricing decisions. People were so outraged, they published Shkreli's personal information in online forums, with some commenters encouraging prank calls, pizza deliveries, and even solicitation of prostitutes to his residence.[3]

Once a doxxing attack has taken place, especially when it concerns public figures and includes inciting language, personal information can spread uncontrollably, making containment nearly impossible without professional intervention.

Stalking and harassment

Accessible personal information becomes even more dangerous when it leads to physical surveillance and obsessive behavior.

This can include:

- Repeated messages or calls
- Monitoring online activity
- Appearing at known locations
- Following family members on social platforms

One of the most alarming examples of this happened to Marissa Mayer, then CEO of Yahoo!. Mayer was stalked by a man who sent her repeated, unwanted, and sexually graphic emails from various locations.[4]

Threats and coercion

Many attacks, especially those directed toward public figures, are preceded by threats. These are often delivered digitally, such as via email, direct messages, forum posts, and social media comments.

Threats should always be taken seriously. They can even be used to predict when escalation to violence is likely to occur. Among other signifiers, the presence of personal details can indicate the likelihood of physical violence.

This can include:

- Referencing home addresses
- Naming family members
- Mentioning schools or workplaces
- Citing past movements or events

Security experts noted that UnitedHealthcare CEO Brian Thompson had received threats related to his role and high public profile, prior to the attack that took his life.[5]

Physical violence

In the most severe cases, digital targeting culminates in real-world attacks.

While not every digital threat leads to physical harm, most physical attacks are preceded by some form of digital reconnaissance, fixation, or signaling.

Apple CEO Tim Cook has been a victim of online fixation that led to threatening behavior and stalking that included trespassing at his home. In early 2020, a woman from Virginia reportedly sent Cook hundreds of emails—some including images of a loaded gun—and repeatedly tagged him on social media, claiming personal relationships and making disturbing threats.[6]

Signs your executive protection program needs a digital layer

If you recognize several of these, digital exposure is likely increasing physical risk

- ☐ You do not regularly audit where executives' personal information appears online
- ☐ You rely primarily on physical security measures (guards, access control, surveillance)
- ☐ You cannot quickly remove executives' personal data from websites, forums, or social platforms
- ☐ You are usually alerted to threats after they escalate
- ☐ You lack continuous monitoring of online mentions and hostile content
- ☐ Your executives or their families have experienced harassment, doxxing, or unwanted contact
- ☐ You have limited visibility into early-stage online targeting or fixation
- ☐ You do not have a defined process for responding to digital threats

A comprehensive executive protection framework

Effective executive protection today requires a structured, proactive approach that addresses both visible and invisible risks.

1. Reduce exposure

The first step is minimizing the information that could make an executive a target. This includes:

- Limiting publicly available personal data across websites, social media, and forums
- Avoiding the oversharing of routines, travel schedules, or family details
- Controlling what employees, contractors, or partners publish about the executive.

Reducing exposure raises the difficulty for potential attackers to gather actionable intelligence. It can often disrupt the early stages of the targeting process, preventing escalation.

2. Detect early warning signs

Once exposure is reduced, the next step is vigilant monitoring:

- Identifying threats in social media posts, forums, blogs, and news articles
- Tracking harassment campaigns or hostile commentary
- Recognizing escalation patterns that indicate an increased likelihood of real-world risk.

Detection allows security teams to intervene before a digital threat evolves into a physical incident.

3. Assess legitimacy and escalation risk

Not every online comment or mention warrants action. A structured assessment process evaluates:

- Credibility of the source
- Specificity of personal details disclosed
- Presence of threats or intimidation
- Context of recent company news, public statements, or controversial decisions.

This ensures resources are deployed efficiently and appropriately.

4. Respond proportionally

Response measures are applied according to assessed risk:

- For lower-risk situations: digital mitigation, removal of sensitive information, warnings, or alerts
- For medium-risk situations: temporary physical adjustments, heightened monitoring, or coordination with law enforcement
- For high-risk situations: immediate intervention, protective deployment, or emergency support.

A proportional approach reduces unnecessary disruption while ensuring safety.

5. Coordinate stakeholders

Modern executive protection is multi-dimensional. Effective programs integrate:

- Physical security teams
- Digital protection specialists
- Legal counsel
- Family or close associate protection.

Coordination ensures that every potential threat is addressed holistically and consistently.

Ironwall delivers digital executive protection

Ironwall transforms the digital bodyguard concept into a comprehensive, actionable solution. By combining prevention, monitoring, and emergency response, Ironwall ensures that executives are protected both online and offline, reducing risk before threats escalate into the physical world.

1. Prevention: removing exposure across the web

Ironwall continuously scans the searchable web to identify personal information about executives and their families. Unlike solutions limited to people-search or data broker sites, Ironwall removes content wherever it appears—from social media posts and blogs to news archives, forum mentions, and cached pages.

Key benefits:

- Reduces actionable information available to potential attackers
- Minimizes the risk of doxxing, harassment, and targeted threats
- Protects the executive's family and close associates.

By proactively removing personal data, Ironwall makes targeting more difficult, stopping many threats at their earliest stage.

2. Monitoring: anticipating threats before they escalate

Prevention alone is insufficient. Ironwall's monitoring capabilities provide continuous threat awareness:

- Detects harassment campaigns, doxxing, and stalking attempts in real time
- Recognizes escalation patterns based on threat intelligence
- Flags periods of elevated risk (e.g., public appearances, major company announcements, and controversial corporate decisions).

This predictive approach allows security teams to respond proactively, rather than reactively.

3. Emergency threat support: rapid, coordinated response

When threats escalate, Ironwall ensures executives are supported with specialized emergency protocols. Ironwall:

- Alerts security teams and law enforcement as needed
- Provides verified intelligence to guide physical protection measures
- Extends protection to all family members (even if not residing together)
- Offers one-on-one support from former LEOs.

With Ironwall, digital intelligence becomes actionable, seamlessly complementing traditional physical protection measures.

4. Expertise you can trust

Ironwall's team is trained by former federal law enforcement officers in threat assessment and the detection of escalation patterns. This ensures that every alert, recommendation, and intervention is informed by real-world security expertise, bridging the gap between digital intelligence and physical protection.

Conclusion

Organizations seeking to strengthen executive protection should consider how digital exposure contributes to physical risk. Ironwall supports executive protection teams with data removal, ongoing monitoring, and emergency threat response as part of its digital bodyguard approach.

See how a digital bodyguard fits into your executive protection program

Explore Ironwall's executive protection

References

1. Evans, Gareth. "Heroism Attributed to Suspect Luigi Mangione Alarming – Mayorkas." BBC News, December 22, 2024. https://www.bbc.com/news/articles/c4gp9ejk40no.
2. Katersky, Aaron. "Executive 'Hit Lists' and Wanted Posters: NYPD Warns about Threats to Executives." ABC7 Chicago, December 11, 2024. https://abc7chicago.com/post/executive-hit-lists-wanted-posters-nypd-warns-threats-executives/15636030/.
3. CNNMoney. "'Most Hated' Pharma CEO's Contact Info Exposed Online." Hartford Business Journal, September 24, 2015. https://hartfordbusiness.com/article/most-hated-pharma-ceos-contact-info-exposed-online/.
4. Slifer, Stephanie. "Homeless Man Accused of Stalking Yahoo! CEO Marissa Mayer." CBS News, March 6, 2015. https://www.cbsnews.com/news/man-accused-of-stalking-yahoo-ceo-marissa-mayer/.
5. Wikipedia contributors. "Killing of Brian Thompson." Wikipedia, December 10, 2024. https://en.wikipedia.org/wiki/Killing_of_Brian_Thompson.
6. Allyn, Bobby. "Apple's Tim Cook Wins Restraining Order against Woman, Citing Trespassing and Threats." KPBS Public Media, January 25, 2022. https://www.kpbs.org/news/national/2022/01/25/apples-tim-cook-wins-restraining-order-against-woman-citing-trespassing-and-threats.