Quarterly Executive Threat Watch

Open-Source Information Report

New Jersey Regional Operations & Intelligence Center (NJ ROIC), Threat Analysis Unit ~ ROIC202512-32981T
NJ ROIC SIN: NJ-TER-0300 (Events); NJ-TER-0400 (Groups/Individuals)/DHS SIN: HSEC 8
January 2026

Scope

The New Jersey Regional Operations & Intelligence Center (NJ ROIC) provides the following assessment of open-source reporting of potential threats to corporate executives for the situational awareness of executive protection professionals. Following the fatal shooting of UnitedHealthcare CEO Brian Thompson and the current political climate, there is a heightened threat environment surrounding corporate executives. Corporations and their executive leadership should remain vigilant of threats and other security concerns.

Current Threat Environment

Corporate executives should remain vigilant of lone offenders with personal grievances. Online glorification of the murder of Brian Thompson and calls for violence are still apparent and further create a risk for a lone offender attack. Public discourse increasingly attributes the challenges faced by the middle and lower classes to the actions and influence of wealthy corporate executives.

According to a September 2025 Allied Universal survey, there has been a surge in threats against corporate executives, with 66% of U.S. security chiefs reporting an increase in threats to company executives. Technology, defense, consumer staples, energy, and pharmaceuticals are the sectors with the largest increase in threats of violence. Allied Universal also reports that misinformation/disinformation campaigns have increased and have the potential to put staff at risk. Additionally, executives who publicly comment on political or sensitive topics have a higher risk of threats.

Due to the growing sophistication of AI, impersonation-based cyberattacks have increased (Cybersecurity Dive). The attacks use increasingly sophisticated voice-cloning and deepfake technology that enables attackers to impersonate trusted contacts and gain privileged access. Attackers exploit that access to deceive colleagues and conduct corporate extortion. These attacks aim to put executives and their families at risk of harm.

- **23 December 2025:** Several far-left groups posted a satirical wish list for Christmas including tools for action and sabotage and home addresses of various CEOs and shareholders. (SITE Intelligence)
- **18 December 2025:** An anonymous user posted to 4chan doxing several high-profile business leaders. The post condemned the global adaptation of digital IDs. (SITE Intelligence)
- **10 December 2025:** Users on X called for the assassination of the Netflix CEOs amid discussions of the company's potential purchase of Warner Bros. (SITE Intelligence)
- **5 December 2025:** 4chan users debated the aftermath of the 2024 assassination of UnitedHealthcare CEO Brian Thompson and the opportunity of copycat attackers. A user wrote, "CEOs deserve to die, and especially the board members/major shareholders, and private equity owners, as well as the offending Congress persons." (SITE Intelligence)
- **16 September 2025:** A far-left forum encouraged activists to campaign against individuals tied to the Copperwood mining project in Michigan. Personal identifiable information (PII) of CEOs, shareholders, politicians, contractors, and public supporters was shared online. (SITE Intelligence)
- **8 September 2025:** A pro-Palestine blog claimed responsibility for vandalizing the New York Times executive editor's apartment. The building was vandalized with blood-red paint and the message, "Joe Kahn Lies, Gaza Dies." (SITE Intelligence)
- **12 August 2025:** 4chan users responded to a 2021 article defending the company BlackRock, prompting an influx of threats against the company. Users proposed targeting other companies including Palantir, Vanguard, and State Street, writing, "Don't care. Everyone employed by BlackRock, Vanguard or Blackstone, their executives, their buildings - everything, everyone needs to be brutally murdered and destroyed. Palantir as well." (SITE Intelligence)

Threats and Vulnerabilities in the United States

- **15 December 2025:** Four members of an anti-capitalist/anti-government group, Turtle Island Liberation Front (TILF), were arrested for plotting attacks using improvised explosive devices (IEDs) against two unnamed U.S. companies. The attacks were planned for New Year's Eve. (DOJ)

- **24 November 2025:** Three people were accused of plotting to kill a businessman from Macomb Township, Michigan, to keep him from pursuing an investigation against one of the defendants. Police were called to a residence following reports of a shooting. (Fox Detroit)
- **3 October 2025:** A man entered the Hudson Yards investment firm, Kohlberg Kravis & Roberts, asking to speak to "the CEO." When ordered to leave, a security guard reported the man ranting, "Kill [name not released] Kill Kill Die Die Die." This was not the first time this individual had threatened executives at the firm. (The Spirit)
- **13 August 2025:** A Galway, New York, man was charged with sending threatening voicemails to the family of UnitedHealthcare CEO Brian Thompson. The defendant expressed satisfaction over the killing of Thompson and stated that Thompson's children deserved to meet the same end. (DOJ)
- **8 August 2025:** The CEO of the Las Vegas real estate firm, Augustus, received a suspicious package containing a severed pig's head and a threatening letter. The letter warned the CEO, "Enjoy your moment while it lasts. And don't get greedy because pigs get fat and hogs get slaughtered." (News 3 Las Vegas)

Recommendations for Corporate Security Officials

Corporate intelligence teams should be proactive in safeguarding high-level executives, as it requires a comprehensive security strategy. The following best practices may help organizations eliminate threats and enhance the overall safety of their executive leadership.

- Increase physical security measures for high-level executives
  - Access to executives should be managed through credentialing and physical security measures
    - Conduct testing of effectiveness of security measures
  - Vary daily routines, including schedules, errands, commutes, parking locations, etc.
  - Exercise caution when leaving or entering areas or spaces
- Sanitize private information found online
  - Limit public disclosure of sensitive information such as location and time of public engagements
  - Train employees on safe online habits and how to enhance personal security
- Flagging and verification of violent threats
  - Encourage reporting of suspicious activity and threatening messages
- Coordinated information sharing between private and public sector intelligence teams
- Implement online personal security practices for executives
  - Remove personally identifiable information (home address, emails, etc.)

Sources: Open-Source Information
Source Reliability: Mostly Reliable
Dissemination: Public/Private Sector
Contact Information: *Any questions about this product should be directed to the NJ ROIC Threat Analysis Unit at* [redacted] *or* [redacted]
Suspicious Activity Reporting: *Suspicious activity with a possible nexus to terrorism, targeted violence, or other related activity should be reported to NJOHSP CTWatch at 866.4SAFENJ (866.472.3365) or tips@njohsp.gov.*