The 3 Critical Areas Where Experts Say Technology is Influencing The Latest Executive Protection Strategies

Physical and cyberattacks are on the rise. According to the Federal Bureau of Investigations (FBI), the most recent data shows an 82% rise in violent crimes from 2017 to 2021. Another study from the FBI reports a 52% increase in active shooter incidents in the same four years, and cybercrimes are also increasing.

In the FBI's 2022 Internet Crime Report, the federal agency received 800,944 complaints – 5% more than the previous year. Moreover, the same report reveals that from 2021 to 2022, the monetary loss grew from $6.9 billion to $10.2 billion.
The security statistics for businesses, specifically for individuals in the C-suite, are on the rise too.

Ontic's Center for Protective Intelligence (CPI) report revealed 206 incidents reported against executive personnel. Most (86%) incidents were physical, and 14% were cyber-related. According to CPI's report, 40% of executives were injured or killed due to attacks.

The executive protection (EP) professionals protecting high-profile business leaders leverage technological advances to enhance their tactical and strategic EP missions. For example, Cindy Marble, Senior Director of Fraud Assessment and Management Operations at Ontic, says technology is a great asset and a liability for EP agents.

"Technology makes our jobs more difficult because information travels at the speed of light," Mable said. "Bad news travels faster than anything. Even so, technology is helping us do our jobs better and faster with more real-time information."

She outlines three areas where technology is improving EP agents' security strategies. The three areas include:
1. The profile of an executive protection professional
2. Incident prevention
3. Internal and external communications

The profile of an EP professional

Technology is changing the profile of an EP agent. A large male wearing a suit, sunglasses, and speaking into his microphone-wired wrist is the stereotype most often associated with a protective agent. While the description is valid, new agents also come with business acumen and technology-based skills.

"People see what they perceive. A person standing next to a principal with sunglasses and a radio speaking into their wrist," Jim Baker, a protective intelligence analyst, said. "We need to break down that stereotype that EP professionals are these big, tall [people]. I'm 5 feet, 3/4 inches tall."

The analyst continued that EP professionals need computer skills to combat the increasing cyber threat against executive leaders.

A report published by Ontic called "Executive Targeting: Analysis into the Protection of Corporate Business Leaders" cited 28 cases of cyber-related incidents targeting executives. (Figure 1) Death threats and CEO impersonations were the two most common types. The most common motive behind the threats was financial gain. (Figure 2).

CYBER INCIDENT

DEATH THREAT	12
CEO IMPERSONATION	11
STALKING	02
STOLEN DATA	01
ACCOUNT HACK	01
PHONE HACK	01
TOTAL	28

Figure 1. Source: Executive Targeting: Analysis into the Protection of Corporate Business Leaders, Ontic

MOTIVE

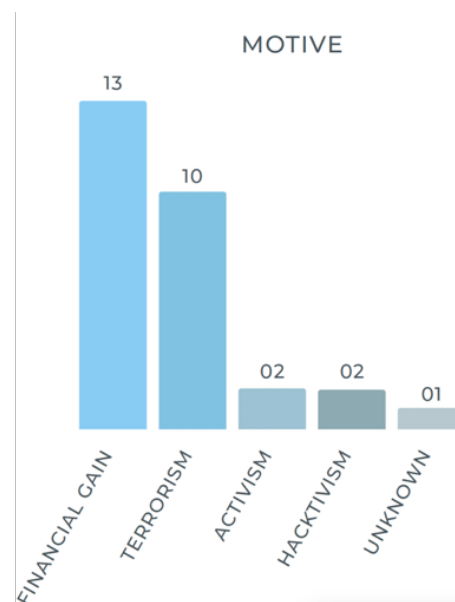| FINANCIAL GAIN	TERRORISM	ACTIVISM	HACKTIVISM	UNKNOWN
13	10	02	02	01

Figure 2. Source: Executive Targeting: Analysis into the Protection of Corporate Business Leaders, Ontic

EP professionals with technical smarts use security-monitoring software to cut out the noise and focus on the most immediate threats.

Incident prevention

Advances in artificial intelligence (AI) and robotics are eliminating millions of jobs. Research reveals that 1.7 million jobs will be lost to automation, and robots will replace an estimated 20 million positions.

Jobs in the EP industry, however, require a human in the role. Even though a physical body is necessary, Technology gives agents a smarter way to prevent incidents against a principal.

Chris Story, Director of Risk Intelligence and Security Consultant at Triumph Protection Group, said, "[Technology] doesn't diminish the role of the individual protector that's standing right next to the person to deal with the unknowns. We're going to use the tools to focus on the true threats and not get distracted by white noise."

For example, an associate director of global security for a Fortune 100 company explained how AI tools, like Ontic, expedite the investigation process to stay ahead of possible threats.

"It took our team just 30 minutes to create a profile," the global security director said. "Previously, we spent almost eight hours assembling research from third-party sources and relying heavily on Google search."

Significant advances in cloud-based security software let EP teams view numerous threats across multiple planes in one central location – saving time and resources.

Internal and external communications

 Universal software technology and consolidated threat intelligence increase collaboration between EP professionals and departments within an organization. Collaboration of these departments also enables holistic data analysis for deeper visibility, speedy decision-making, and clear communications across multiple functions.

"Technology is a multiplier for the protector," Story said. "Layering those concentric security rings with technology to better support solo protection."

Former U.S. Secret Service Agency John Gullickson explains that Technology also helps communicate what a security team does for the company's leaders and employees, along with why they do it.

"Socializing what you're doing with everyone around you," Gullickson said. "It's important to talk to them and explain why you're there because it's not just about protecting the CEO or leaders. It's about protecting them at an event."

Communicating security protocols across an organization is vital to the successful protection of the principal too.

"We develop counterparts by getting people to understand what we do and actually letting them know that we need them," Ontic's Cynthia Marbles said. "Whether it's human resources, the legal team, or even the executive's gatekeeper, we want them to be our counterparts to give us the information so that we can do our jobs better."

CTA IDEA - DEMO?