AGENDA

‘Very Scary Reality’: Boards Need to Review Exec Security Procedures After Shooting

Boards can’t "set it and forget it"

By Nick Muscavage | December 9, 2024

Business leaders have been reaching out to security service providers to inquire about executive protection in the wake of the murder of UnitedHealthcare CEO **Brian Thompson** in Manhattan.

Thompson, 50, was fatally shot outside of a Hilton hotel in midtown Manhattan on the morning of Dec. 4 by a hooded man wielding a silencer-equipped pistol. The CEO was in New York for **UnitedHealth Group**'s investor day and reportedly had no security detail when he was shot despite known threats against him, according to reports. On Monday, police in Altoona, Pa., arrested 26-year-old **Luigi Mangione**, of Maryland, in connection with the shooting following a tip from a **McDonald's** employee.

Boards should be reviewing their security needs on a regular basis and, if the need is there, consider expanding personal security perquisites to named executive officers other than CEOs, sources said. Some security perks may be qualified as a nontaxable benefit for the executive and could be eligible for a tax deduction by the company, according to sources.

Crime scene investigators in Manhattan investigating the fatal shooting of UnitedHealthcare CEO Brian Thompson on Dec. 4, 2024. Source: Getty.

There's been a flood of interest in executive security since Thompson's murder, according to **Jeremy**

Baumann, founder of **Corporate Security Advisors**, a consulting firm that helps companies craft security programs.

"It's certainly been a busy couple of days for anyone in the corporate security world, whether they're the service provider in this space or on the inside of an organization," he said. "The high-profile nature of this event has hit the desk of executives and boards across the country."

Thompson was CEO of UnitedHealthcare, the health insurance division of UHG. While he wasn't the top executive at the health care behemoth, he was a named executive officer in the company's proxy statements.

When exploring security options for high-ranking employees, it may be a good practice to apply a risk-based approach to gauge the protection needs throughout the C-suite as well as the executives a rung below, according to **Ken Senser**, chief strategy officer at Corporate Security Advisors and formerly a senior vice president at **Walmart** handling global security.

"In a truly risk-based program, you may find that the actual risk is to officers that are not named executive officers but are further down in the structure yet are heading organizations that generate friction," he said.

While there may not be a security need for the CEO, a group president "may warrant something more than just the standard for workplace protection" if they are in a position that could garner threats, Senser said.

By the Numbers

Last year, 109 companies, or about 21%, of the S&P 500 included personal security as a perk for executives, according to data from public company intelligence provider **MyLogIQ**. Most of these perks (49) went to CEOs, followed by CFOs, who received 14 of these perks.

While the majority of these perks were in the C-suite, 16 personal security benefits went to presidents and vice presidents who did not hold C-suite roles, according to the data. The **Securities and Exchange Commission** requires security perquisite disclosures only if they are for the executive's personal use and not during ordinary business.

These perks are taxable income because they are considered benefits to executives. However, certain services, such as personal security or private transportation, can be excluded from an executive's gross income if it qualifies as a "working condition fringe"

under the Internal Revenue Code's Section 132, according to **Christine Tsai**, a senior associate in **Pillsbury's** tax practice.

"To qualify, this generally requires a bona fide business-oriented security concern for the employee, establishment of an overall security program by the employer, and adequate documentation to substantiate the security assessment," she said. If the benefits qualify, a company can generally deduct the costs as a necessary business expense from its taxes, she added.

If boards consider upping the personal security of executives following Thompson's death, it's possible shareholders will scrutinize the increased costs. However, investors typically support the use of such perks, so long as there is a reasonable explanation for them, according to **Stephanie Hollinger**, vice president at **ISS-Corporate**.

Shareholders "generally have maintained their support of the use of perquisites, but outsized values or perquisites utilized without compelling rationale may draw increased scrutiny prompting compensation committees to carefully consider the cost and benefits," she said, adding that a detailed disclosure may be necessary if the value of the benefit is significantly higher than the market norm.

To view the graphic, click here or go to https://www.agendaweek.com/c/4707014/627934?referring_content_id=4707014&referring_issue_id=627934

The practice of covering home security as a perk has increased steadily over the past five years, according to an analysis from ISS-Corporate. In 2019, about 12% of S&P 500 firms paid for the home security of executives; in 2023, that number increased to around 16%, according to the data.

The analysis found that health care and insurance was one of the industries with the highest prevalence of personal security benefits, but those numbers still sat 5% and 6.3% of their respective industries. Financial services had the most widespread practice of providing personal security, with 11.3% of the industry supplying this perk, followed by media and entertainment and capital goods, which both had 8.8%.

'You Can't Put a Price on a Life'

Companies outside of the industries where this is a common practice have begun reaching out to security consultants, according to **Glen Kucera**, president of enhanced protection services at **Allied Universal**, which provides executive protection

Related Content

August 19, 2024
High-Profile CEOs See Security Perks Climb in Divisive Environment

July 24, 2023
Musk Vs. Zuck 'Cage Match' Gins Up Key Person Risk Concerns

Allied has been contacted over the past several days from companies inquiring about security risk assessments, social media monitoring and executive protection, and they weren't all insurance companies, Kucera said.

"I think companies, regardless of what vertical or industry they're in, are going to start making these initial considerations," he said.

However, insurance companies may feel that need more intensely, he said.

"When it comes to the health care business ... all of these decisions are either impacting quality of life or life and death," Kucera said. "So, when that decision is made and it doesn't go somebody's way, they become very emotional and those emotions are what make people act out."

CEOs at all companies make decisions that are contentious at times, he said, adding that companies should monitor the safety of key personnel against threats internally and externally.

Larger companies may perform these assessments through in-house security teams, but many companies contract these services out to third parties, according to **Brittney Blair**, a senior director at risk advisory firm **K2 Integrity**.

Security assessments should include online monitoring not just of social media but also of the deep web, she said. They should also assess risks of events and travel. If a threat is severe enough, it should be elevated to the board.

"The board has to make informed decisions regarding security expenditures and potentially upping the security expenditures," she said.

One challenge boards may face when exploring the expansion of security costs is resource allocation, Blair said. Boards need to recognize that while there may not be a direct return on these investments, they are still crucial, she said.

"You can't put a price on a life," she said.

Companies should be reviewing their security assessment procedures at least once a year to see what needs to be adjusted, but many companies "set it and forget it," she said.

These assessments can also be done when a major change is occurring at a company, such as a restructuring, Kucera said.

Meanwhile, some firms in the S&P 500 disclosed covering personal cybersecurity perks for executives, including identity theft prevention, in proxy statements.

In light of Thompson's murder, cybersecurity protection of executives should be an area of renewed focus, according to **Brian Finch**, a partner at **Pillsbury**. This is because cybersecurity "is a personal protection issue as well," he said.

"If you get access to those devices, you will know someone's schedule, you know their agenda, their travel plans, their movements, and you can track them that way," he said.

While there are best practices to follow to reduce risk, "there's no such thing as perfect security," he said.

Still, these discussions are likely to become more prevalent in the boardroom and C-suite.

Proactive monitoring and regular security assessments are needed to stay ahead of threats, Blair said.

"This horrible situation was maybe the wake-up call for a lot of people to see that very scary reality," she said.

Editor's note: This story has been updated with emerging information about the case.