ALM | LAW.COM

CORPORATE COUNSEL

Recent CEO Shooting Tragedy a Reminder for Corporate Risk Assessment and Incident Response Plans

December 11, 2024

The tragic fatal shooting of UnitedHealthcare CEO Brian Thompson on December 4 in Midtown Manhattan shocked the nation—and especially the business and corporate community—with its brazenness, coldness, and cruelty. Beyond just this single incident, recent news suggests that executives and senior politicians have been increasingly targeted for violence as of late, with President Trump having been targeted by the Iranian government and members of his transition team having received bomb threats.

These and other events serve as a powerful reminder of the need for crisis management response plans. And, specifically, they have left the political branches as well as corporate America reassessing the need for executive security to try to prevent similar incidents from happening in the future. In an era when executives' movements (including flight travel) can be tracked more easily than ever and social media and the internet have increasingly been used to channel anger towards businesses, this renewed focus on safety may be more than justified especially when viewed under the penumbra of the business judgment rule.

Photo: Stefan Jeremiah/AP

Members of the New York police crime scene unit investigate bullets lying on the sidewalk at the scene outside the Hilton Hotel in midtown Manhattan where Brian Thompson, the CEO of UnitedHealthcare, was fatally shot, Wednesday, Dec. 4, 2024, in New York.

Given the current state of affairs as well as the overall framework for corporate and director and officer liability, corporations would also do well to ensure they conduct robust risk assessments of officer security and prepare incident response plans to follow in the event the unthinkable happens—whether at a company's headquarters, other onsite locations, or just in general.

To be clear: We realize that this is a highly sensitive topic and emotions are running high. We are keenly aware that many are mourning the loss

of a loved one, friend, colleague, and boss. But if history in the crisis management area teaches anything, it is that in moments of crisis—when a surprise event or attack descends—the time for action becomes now, not later. It is in that spirit we enter the fray to speak about a critically important topic that needs present and future attention. After all, as leaders, we must all "stand in the storm" and choose "courage over timidity."

Corporate Sources of Liability

The many sources of liability for corporations and those who run them are familiar and often include areas of focus such as tax avoidance and evasion, foreign and domestic bribery, insider trading, fraud, trade secret theft, just to name a few. The Department of Justice and the Securities and Exchange Commission, among the many other federal and state agencies, are charged with investigating and prosecuting potential corporate wrongdoing, including by individual employees, officers, and directors. Private securities lawsuits against corporations are also common, including when corporate events are followed by a drop in stock price. And, of course, all officers and directors have fiduciary duties towards their companies, including duties of care, loyalty, good faith, confidentiality, and disclosure.

In addition, courts have found that directors and officers have a duty of oversight and may be liable for their "inattention" or "negligence" towards "liability-creating activities within the corporation."Alleged breaches of these fiduciary duties can result in shareholder derivative lawsuits brought against directors and officers on behalf of the corporation. Indeed, in recent years, many of these derivative lawsuits settled for hundreds of millions of dollars, including suits related to corporations' failure to prevent financial statement errors, bribery, self-dealing, sexual harassment, or improper business practices.

Thus, corporate directors and officers must exercise care to investigate corporate risks and be prepared to address them. This includes the need to have a reporting system that ensures material relevant information about risks reaches the board level, where appropriate, and to respond to "red flags" regarding potential problems within the company. So, for example, if a corporation has received a threat against a particular officer, directors and officers may have heightened duties to follow up on that threat and take appropriate precautions.

The Need for Security Risk Assessments & Incident Response Plans

Crisis management response plans take on many forms and include both a preventive component as well as an action plan in the event a dreaded risk materializes. In the context of officer and director security and well-being, officers and directors should ensure that key executives and other personnel have been identified and that processes are in place to make sure that threats against those persons are captured, monitored, investigated, and elevated (including to law enforcement) where appropriate. Such processes and procedures must also include a way to preserve potentially key evidence. Indeed, the preservation of evidence in a threat context may well be so paramount as to warrant the exclusion of such threats and their associated materials and assessments from a company's ordinary document destruction policy.

Even in situations where threats are viewed and ultimately treated as remote and not requiring further action in relation to the likely costs and other resources of additional officer security (which must be disclosed to shareholders as a "perk" under SEC rules), the fact remains that just as with any other informed decision, boards and committees cannot make that assessment without the appropriate information. In this regard, qualified in-house or outside investigators,

consultants, and legal counsel can advise boards about the contours of an appropriate risk assessment and incident response plans.

Legal Privilege & The Self-Critical Analysis Doctrine

Importantly, when done by counsel under the auspices of the provision of legal advice, such assessments can be protected by the attorney-client privilege. However, counsel (especially in-house counsel) must be careful to ensure that their work is regarded as legal in nature—*i.e.*, for purposes of providing legal advice—to avoid challenges down the road that the communications and other related work product are not entitled to protection. As many in-house attorneys may recall, under the "primary purpose" doctrine, privilege may apply to communications with attorneys that have both a legal and a business purpose, but only if legal advice is the (or a) "primary purpose." But even without the involvement of legal counsel, all is not lost. Perhaps more generally, the self-critical analysis privilege can also provide fallback protection in certain jurisdictions even in the absence of counsel. Specifically, although not universally accepted nor applied, at its core, the self-critical analysis doctrine seeks to "protect the opinions and recommendations of corporate employees engaged in the process of critical self-evaluation of the company's policies for the purpose of improving health and safety."

Individualized Assessments and Plans – No "One Size Fits All"

Thus, boards and their committees should be prepared with incident response and succession plans addressing potential attacks on executives, just as they would have plans to address other key threats to operations. These plans should not be "one size fits all," but take into account the specific facts and circumstances of the industry, the corporate profile, the political landscape (whether local, regional, national, or international) the impacted executives, as well as the location and geography of the executive(s) and company. Again, legal counsel whether in house or outside, can work carefully with security consultants, investigators, and others to develop such plans under the protections of the attorney-client privilege.

The UnitedHealthcare shooting was both horrifying and tragic. It sent—and continues to send—shockwaves through the professional community. We are sensitive to that and realize that many are, too. But in the same way that many people delay or avoid putting in place a final will and testament, the killing served as a painful reminder among professional circles and others of what best practices companies and their senior leadership teams, including executives, boards, and committees, should put in place now in the event of an "unthinkable" tragedy later.

At bottom, companies and those who manage them have an obligation to prepare for the worst threats to their businesses, even as they work to keep them from materializing. Robust risk assessments as well as incident response and succession planning for executive security breaches should be part of every company's DNA. And, for the reasons already discussed here, ideally, in consultation with in-house or outside counsel serving in their capacity as legal advisors with experience handling crisis management situations.

Andrew S. Boutros *co-chairs Shook, Hardy & Bacon's Government Investigations and White Collar Practice.* ***Jay Schleppenbach*** *and* ***Stuart W. Risch*** *are partners in the firm.*