LAW360

Portfolio Media. Inc. | 230 Park Avenue, 7th Floor | New York, NY 10169 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

When Physical And Cyber Threats Converge: 6 Tips For Cos.

By **Matthew Harden, Micaela McMurrough and Arlo Devlin-Brown** (May 8, 2025, 11:58 AM EDT)


Matthew Harden


Micaela McMurrough


Arlo Devlin-Brown

The first few months of 2025 continued the disturbing trend of an increase of digital threats made against corporations, organizations and high-profile individuals.

This trend, of course, follows the December 2024 fatal shooting of UnitedHealthcare CEO Brian Thompson, and a corresponding rise in vitriol on the internet and dark web following the incident, including the proliferation of "Most Wanted" card decks targeting high-profile executives and individuals.

In reality, however, the targets of these threats span everyone from senior corporate executives to celebrities to nonexecutive employees. Employers, in particular, should be tuned in to how threats against — or by — employees can affect the corporate workplace. While there is no one-size-fits-all response, it is increasingly important for companies to consider a multifaceted approach to enterprise risk management to identify, assess, mitigate and respond to digital threats.

Alongside these rising threats, there has been a continued emergence of a legal framework for how corporations, organizations and other entities are expected to respond to these digital threats.

This developing legal landscape provides a road map for general counsel and their teams to navigate the increasingly fraught landscape of digital threats and to manage risks to their executives, employees and other stakeholders.

Convergence of Physical and Cyber Threats

As Flashpoint observed at the end of 2024, threats of harm are no longer confined to the physical or virtual spaces: "Executives and high-profile individuals are increasingly targeted both online and offline," requiring organizations "to address the convergence of physical and cyber threats."[1]

We have described this convergence as a rise in digital threats.

Cyber tools have increased the attack surface for those launching digital threats — threatening and harassing communications may arrive by email, phone call, text message or social media — and, increasingly, may leverage emerging tools, like generative artificial intelligence and deepfakes.[2]

At the same time, cyber vulnerabilities have enabled attackers to develop detailed and sometimes real-time information about targets. For example, prior data breaches and dark web marketplaces have expanded the availability of compromised personal information that may facilitate real-world harms. Additionally, phishing techniques and other social engineering may provide real-time access to sensitive devices and information, like calendars and location data.[3]

The convergence of physical and cyber threats necessitates a multifaceted approach to enterprise risk management to identify, assess, mitigate and respond to digital threats.

Emerging Legal Guidance

As a matter of federal statute, Title 29 of the U.S. Code, Section 654(a)(1), requires employers to provide employees with a place of employment that is "free from recognized hazards that are causing or are likely to cause death or serious physical harm." However, there are no specific Occupational Safety and Health Administration standards regarding workplace violence.

Instead, guidance regarding legal expectations for responding to digital threats has emerged mostly from judges resolving common law claims and state statutes imposing affirmative obligations on educational entities, which provides persuasive guidance for other entities navigating similar risks.

As a matter of common law torts, employers may owe their employees — and sometimes others — a duty to take reasonable precautions against threats of violence by third parties. The existence of a duty typically depends on the existence of a special relationship between the employer and the affected person, and whether the criminal acts at issue were foreseeable. An employer-employee relationship generally qualifies as a special relationship, and where the duty exists, an employer must act reasonably under the circumstances.

In the absence of specific, forward-looking guidance, common law precedent provides backward-looking guidance on whether certain responses to threats were reasonable. For example, some cases have provided benchmarking on when warnings or other precautions may be warranted.

On Sept. 26, 2024, in Wu v. County of Los Angeles, the Court of Appeal of the State of California, Second Appellate District, advised that the state defendants had a duty to warn campers staying at a state park about a shooting threat when they had already warned their own employees.[4]

Similarly, on March 25, 2022, in Cleveland v. Taft Union High School District, the Court of Appeal of the State of California, Fifth Appellate District, held that a school threat assessment team had breached their duty of care by, among other failures, not properly communicating among themselves about a threat.[5]

In addition, the passage of some recent state laws requiring educational entities to implement threat assessment programs provide further guidance about what might constitute a reasonable response to digital threats. For example, since 2020, at least 10 states have enacted or amended statutes requiring schools or other educational entities to establish programs for responding to threats.[6] At least two states — Michigan and Vermont — have enacted laws in the first few months of 2025.[7]

The depth of these statutes vary, but many impose specific requirements for preparing for and responding to digital threats, such as requirements to establish multidisciplinary threat assessment teams, develop threat management policies and playbooks, train assessment teams, and disseminate

training and guidance to others in the organization.[8]

Although these statutes typically govern educational entities like schools, they have helped to inform emerging legal guidance for preparing for, evaluating and responding to digital threats by other organizations, particularly those that interact with the public.

In addition, California has enacted — and some states have proposed — requirements relating to workplace violence prevention, including requirements to implement a workplace violence prevention plan and to provide training on the plan.[9]

Together with common law precedent, these state statutes have begun providing a general framework for responding to digital threats.

Actions to Mitigate Legal and Enterprise Risk

In light of the rise in digital threats, along with emerging legal guidance about how to respond reasonably to these threats, general counsel and security teams can look to the following actions, among others, to help mitigate legal — and very human — risk to their entities, executives and workplaces.

Conduct a risk assessment.

Identify the most likely types of threats facing the organization, taking into account the potential effect and likelihood of known or suspected threats.

Create policies, plans or playbooks.

Establish an enterprise approach to identifying, preventing, protecting against and responding to digital threats. A documented approach may help to categorize, assess and appropriately respond to digital threats as they emerge.

Engage a multidisciplinary team.

Bring together a multidisciplinary team to assess, manage and respond to digital threats, including representatives from physical security, information security, human resources and legal.

Consider whether it may make sense to retain outside resources, such as an outside behavioral threat assessment professional with experience evaluating the potential risk of harm, or a threat intelligence vendor with capabilities to monitor for threatening communications.

Exercise the plan.

As with traditional cybersecurity risks, practice the enterprise approach to responding to digital threats through tabletop exercises or group training opportunities. Incorporate lessons learned from these exercises into the organization's policies, plans or playbooks.

Train others and increase awareness.

Spread awareness of potential risks among employees, including by implementing mechanisms to

facilitate effective and efficient reporting of potential or suspected threats, and by establishing employee resources to help prevent or mitigate such threats.

Develop relationships with law enforcement.

Establish relationships with local and federal law enforcement, who may be able to intervene or act as a point of escalation for digital threats. Digital threats may ultimately cross into criminal activity within the jurisdiction of law enforcement authorities.

Conclusion

As digital threats present a heightened risk to organizations, their executives and the workplace, general counsel may look to emerging legal guidance to help prevent and mitigate harms from these threats.

With the convergence of physical and cybersecurity threats, it is increasingly important to consider a multifaceted approach to enterprise risk management to identify, assess, mitigate and respond to digital threats. While there is no one-size-fits-all response, common law precedent and recent state statutes provide a road map for addressing these risks.

Matthew Harden is an associate at Covington & Burling LLP.

Micaela McMurrough is a partner and co-chair of the global and multidisciplinary technology group, and the artificial intelligence and Internet of Things initiative, at the firm.

Arlo Devlin-Brown is a partner at the firm.

Covington of counsel Carolyn Rashby contributed to this article.

[1] Executive Protection in a Volatile Threat Landscape: 4 Key Takeaways from Flashpoint's Intel-Led Community Call, Flashpoint (Dec. 19, 2024), https://flashpoint.io/blog/executive-protection-4-key-takeaways-community-call/.

[2] Julie Jargon, The Panicked Voice on the Phone Sounded Like Her Daughter. It Wasn't., The Wall Street Journal (Apr. 5, 2025), https://www.wsj.com/tech/personal-tech/the-panicked-voice-on-the-phone-sounded-like-her-daughter-it-wasnt-8d04cbc1?msockid=0a5a9bb24e79677b1b648e084f6066e8.

[3] Julian Hayes II, The Invisible Threats to Executive Security Leaders Can't Ignore, Forbes (Mar. 10, 2025), https://www.forbes.com/sites/julianhayesii/2025/03/10/the-invisible-threats-to-executive-security-leaders-cant-ignore/.

[4] Wu v. Cnty. of Los Angeles, 2024 WL 4313638, at *10 (Cal. Ct. App. Sept. 26, 2024) (unpublished) ("[T]he point at which the State defendants determine their own employees' safety is at risk is also the point at which they have a duty to warn campers that their safety is at risk as well.").

[5] Cleveland v. Taft Union High School District, 76 Cal. App. 5th 776, 810 (Ct. App. 5th Dist. 2022).

[6] 105 Ill. Comp. Stat. Ann. 128/45; Mich. Comp. Laws Ann. § 380.1308e; N.C. Gen. Stat. Ann. § 115C-105.65; N.J. Stat. Ann. §§ 18A:17-43.4, 18A:17-43.5; Ohio Rev. Code Ann. § 3313.669; 24 Pa. Stat. Ann. § 13-1302-E; Tenn. Code Ann. § 49-6-2701; Tex. Educ. Code Ann. § 37.115; Va. Code Ann. § 22.1-79.4; Vt. Stat. Ann. tit. 16, § 1485.

[7] Mich. Comp. Laws Ann. § 380.1308e; Vt. Stat. Ann. tit. 16, § 1485.

[8] See Va. Code Ann. § 22.1-79.4.

[9] Cal. Lab. Code § 6401.9 (defining "threat of violence" to include digital and online conduct); Va. H.B. 1919 (2025).