ALM | LAW.COM

'A New and Emerging Threat': Covington's Ashden Fein and Micaela McMurrough Explain How to Brace for AI-Fueled Cybersecurity Risks

By Kat Black
July 24, 2025

Since the COVID-19 pandemic hit in 2020, companies have become increasingly focused on a rising surge of insider and digital risks in the remote workplace—and as artificial intelligence and other emerging technologies become more sophisticated, these concerns have only amplified in the five years since.

Law.com caught up with Covington & Burling partners Micaela McMurrough and Ashden Fein to learn how companies can strengthen their risk management frameworks in the wake of new AI-powered cyber threats.

When did AI's role in cybersecurity threats start becoming top-of-mind for companies and the firms that represent them? Why now?

McMurrough: From the perspective of what we're calling digital threats, the reason that this is important now is because what we're seeing is really the convergence of cybersecurity issues with physical security issues as it relates to individuals and personal threats of harm.

Over the last few years, we've seen this convergence of these two, where bad actors who used to be purely at arm's length can now make very personal threats of harm based on, number one, information that may be available, for example, on the dark web or elsewhere as a result of prior cyber incidents or collection of data across platforms, etc. And then the physical security component where, again, these individuals who used to be at arm's length now may have enhanced information about someone's location, where they're going to be, where they are.

Courtesy photos

Micaela R.H. McMurrough (left) and Ashden Fein of Covington & Burling

And that can be related to collection happening on devices, or it can be related to publicly available information being married up with other sources of data. And so you have this convergence of the cyber threat and the physical security threat to individuals.

I think the biggest example, and the reason why this has been front-of-mind for the last several months, is the [assassination of the] UnitedHealthcare CEO and the related coverage of that issue on the internet, the proliferation of threat information and threat chatter about individu-

als. We saw things like card decks being made where individuals were targeted as "most wanted" targets, those kinds of things. So a a lot of this information that has been out there for a while is suddenly becoming really relevant in connection with this physical security threat.

The other piece I would add on the physical security, personal harm side is that the bad actors are not only taking advantage of this data that is out there, but also of these emerging technologies. So for example, AI and generative AI have allowed these bad actors to craft really specific customized outreach communications that do not have the typical indicia of fraud, such as grammatical errors, punctuation errors, capitalization problems.

And you couple that with the amount of personal information that can be included in these messages, and you can see why bad actors are getting better at getting to their targets ... convincing people that they are somebody that person should know or have some connection with historically. So it's really the convergence of these technologies at this moment in time that we're seeing this uptick in interest in this physical security/cybersecurity threat.

What are the legal frameworks that both exist and are developing to address these issues and mitigate risk, especially given the role of emerging technologies like AI?

McMurrough: When it comes to developing the framework for response to digital threats, there is a lot of common law precedent, and there are state laws out there that in many cases are not directly on point, but you can look to those to try to understand the duties that companies might have to employees, members of the public, third parties, etc. So it really comes down to this question of duty: What duties does this entity owe to these other parties, if any? And that goes to issues that have been discussed in the law for quite some time, such as whether any special relationships exist, etc. But generally speaking, we do see a duty to take reasonable precautions against threats of violence.

So even though there is this idea of duty out there, I think companies still have to put frameworks around what that means to them when it applies, when it doesn't apply, and under what circumstances. So, as often happens in the law when you have a new issue, there may be some existing guidance and precedent out there that you can look to. But this is a new and emerging threat. And so what is expected is not always clear in terms of legal duties and responsibilities.

Fein: Even though not clear, depending on the impact, there could be ... existing frameworks that are applicable. So what comes to mind is heavily regulated industry. Many organizations may not think about insider risk as a type of risk that would trigger such obligations like breach notifications or cyber incident reporting obligations, because they think of those more as like external threats, intrusions. But the reality is that, depending on the industry, depending on the regulator, depending on the framework at play, the definitions of cyber incidents or reportable events could be broad enough to include those events that have certain consequences that are related to insider threats. So the easiest example that comes to mind is in the defense space, where the obligations for U.S. defense contractors are very broad when there is unauthorized access to data or systems. And that could include employees. So where the current frameworks are generally thought of as preventing external intrusions, the cyber threats, the insider threats could also trigger the same sort of obligations to both safeguard and report if there is an incident.

In the event of one of these cybersecurity breaches, what legal repercussions might an employer or company face?

McMurrough: Here, it's not entirely clear what legal repercussions or liability they can face,

because we don't have settled law on a lot of these areas, particularly as it relates to some of these threats or circumstances and how they intersect with the emerging technologies. But companies that face these security issues may face, for example, negligence claims. They may face wrongful death claims. ... There could be tort claims out there. They may also face investigations or potentially enforcement actions from regulators relating to various legal frameworks, depending on the industry or the context.

Depending on, again, the industry or the company and the relationship between the company and the individual or individuals who are harmed, there could be different rules that are on point. So this can be complicated for companies to navigate. On top of that, you want to overlay, for example, in the employer-employee context, existing regulations and frameworks. So for example, OSHA may come into play for some of these circumstances in the employer-employee context.

How can companies or employers prepare for these risks, and how would you advise them?

Fein: Even if the area of law is emerging in many cases, certainly organizations can prepare [by], first and foremost, really taking one's temperature about how they're postured to deal with the particular types of risks, whether it's an insider risk or even more broadly an external cyber intrusion, physical harm and the like. That could be accomplished by conducting a risk assessment internally, bringing in experts to help conduct a risk assessment. ... But it's really trying to gain an understanding of where the organization's current posture is and where the different tension points or risk points are, should there be an incident. That way they could have programmatic solutions that hopefully resolve or mitigate those risks.

Other areas, once those are identified, is to create policies and playbooks to help resolve and respond to issues as they materialize. ... Who should be on a team if there's an insider, who should be the one responding if you find out that you may have [an incident where North Korean operatives are applying for IT roles in U.S. companies], or you just have an individual who departed the company and left with intellectual property—highly valuable—who's that multidisciplinary team? What litigator can run, essentially, to the courthouse and file a temporary restraining order? Which cyber expert, internally or externally, is going to be used to conduct the forensics of that employee or user who left? Which employment law or HR person and/or supporting lawyer is going to support the off-boarding of the individual if they haven't left the company, or if they've left, help with the benefit side to potentially claw back certain benefits in order to incentivize an individual working with the company for an investigation?

Ideas about how to develop relationships with law enforcement, and understanding the different requirements we just spoke about. So a lot of that could be done upfront, ahead of any particular incident occurring, so long as organizations, again, start with identifying where their risk points are and what type of medications they should have in place to resolve them.

McMurrough: Conduct a rehearsal, conduct a tabletop exercise, do a run-through of the playbook and see if the processes that you've outlined reflect where you want to be and best practices for your company. And then the last thing I think I would underscore is just training and training employees about these risks so that they are better able to spot them and report things as they arise.