Key Takeaways

Skadden

Private Equity CISO Fireside Chat: Cybersecurity Leadership in the Age of Generative AI

November 3, 2023

If you have any questions regarding the matters discussed in this memorandum, please contact the following attorney or call your regular Skadden contact.

David A. Simon
Partner / Washington, D.C.
202.371.7120
david.simon@skadden.com

One Manhattan West
New York, NY 10001
212.735.3000

1440 New York Avenue, N.W.
Washington, D.C. 20005
202.371.7000

Speakers: David Simon, Bethany De Lude and David Stern

Partner and co-head of Skadden's Cybersecurity and Data Privacy practice David Simon recently sat down with two chief information security officers (CISOs) from the private equity sector as part of the firm's National Cyber Awareness Month series. Bethany De Lude is a managing director and CISO at the Carlyle Group, and David Stern serves as CISO at KKR. The discussion, "Cybersecurity Leadership in the Age of Generative AI," focused on the emerging challenges surrounding generative AI, as well as the evolving hybrid role of a CISO.

David Simon: We're at an inflection point when it comes to CISOs and their rapidly evolving roles. Companies are expecting CISOs to protect the enterprise, their products and their people. Meanwhile, regulators are increasingly expecting more from management teams and CISOs. For example, the CISO of SolarWinds was served with a Wells notice, which means they're being investigated by the SEC. We also could cite Uber's CISO who was investigated, indicted and then convicted of a crime in connection with a cybersecurity incident, which largely took place before he held the job. What would you both say is the role of the modern CISO, and how has it changed in the last few years?

Bethany De Lude: There's increasing pressure on a modern CISO to wear multiple hats in order to successfully navigate a range of changing environments. First, there's the regulatory environment. State, federal and global data privacy and security regulatory frameworks create a complex tapestry of complimentary and conflicting expectations that need to be considered in structuring a security program. Next, the threat environment continues to evolve both in sophistication and scale, making the CISO's operational hat essential. The modern CISO has to make sure that cyber hygiene is robust, because a lapse in cyber hygiene will equal a successful data breach. Then there's the strategic hat. A successful CISO lifts cyber out of IT to create a horizontal thread that cuts across all areas of the business to manage regulatory, financial and brand risks, and to continue managing operational risk.

David Stern: Being a CISO is hard. You and your organization are the prime targets. These things can certainly happen — the SEC doesn't have to give me a Wells notice to examine me in depth and ask me about everything I've done, or everything my predecessor has done. A CISO has to have a certain mindset and recognize that we're in a dangerous place and at the frontline. If you can't handle that, you should probably be doing something else. But the number one job today for the modern CISO is making sure

that everybody understands their part in the whole cyber program. It's our job to keep everyone honest and educated. It's also about awareness. Management needs to be aware of any critical vulnerabilities in our systems that we may potentially be exposed to, and they need to know that we are working on the issues.

David Simon: It looks like in some ways the big-picture story is perhaps a lack of alignment on issues of corporate governance. What factors should a company consider when determining the reporting line for the CISO? Should the CISO report directly to the CEO, the chair, the COO or somebody else in IT?

David Stern: I think a modern CISO can best do their job with the chief legal officer, specifically in making that person appreciate what the CISO is doing. The same goes for the risk officer and the operations officer — I don't think a CISO should go directly to the CEO or the board. There have to be strong internal relationships that are regularly curated. It's also vital that a CISO is able to gauge the distance their message is going and make sure it's being picked up by the right people. If it's not, then it should be a priority to fix that.

Bethany De Lude: Unless your CIO has a strong cyber foundation, I prefer a reporting line that is outside of the CIO's purview. But I completely agree with David that your number one business partner is typically going to be your technology department. Wherever the CISO sits, it can be really helpful to have some type of security steering committee that pulls in leaders from across your company to provide collective, diverse perspectives; business buy-in; and leadership buy-in that's autonomous to the tech function. Having this type of influential advisory board to inform, carry and reinforce your messaging is a game changer.

David Simon: What about the interplay between cyber governance and AI governance? Do your security committees have purview over generative AI? How does this affect the role of the CISO now?

David Stern: We leveraged our cross-functional risk committees to pivot right into it and bring it on. Generative AI is extremely exciting — we want to put energy into it. We want to get the most out of it that we possibly can. At the same time, we're going to be conscious of risk management. It's a carrot-and-stick sort of thing — I refuse to block new developments for the sake of blocking them. Our committees were able to push back on people who wanted generative AI completely blocked to show how governance, transparency and innovation can all come together to manage that risk.

David Simon: In the aftermath of the Colonial Pipeline incident, which involved ransomware and the closing of critical infrastructure in the U.S., there was suddenly a new focus on the national security implications of ransomware. One of the resulting changes that seems to be emerging from this is the Cybersecurity Infrastructure Security Agency's (CISA's) developing role as an actual regulator. How are you navigating this, and how should CISOs be thinking about it?

Bethany De Lude: It's really tricky because the whole carrot-stick paradigm is muddied right now. We all understand the shared desired outcome, and that's to reduce the likelihood and impact of a cybersecurity incident. We all know that every time an extortion payment is made, criminal enterprises and nation-state actors have essentially received financing to victimize someone else. We all understand that cyberhealth is more than just a company issue — it has to do with national security, economic viability and competitiveness in the marketplace when intellectual property is being stolen. If you were to ask for help from CISA, the FBI or other government entities, and you end up getting both help and an enforcement action, it really puts companies in a difficult spot. No one's figured out how to incentivize the behavior and outcome that we all want in a way that is practical. There seems to be some disconnect in the approach from a policy perspective, so it's tricky right now.

David Simon: The changing role of government partners is definitely something to watch. Let's focus for a moment on the private equity context specifically. We mentioned the Colonial Pipeline incident, as well as the 2020 SolarWinds incident, where several U.S. federal agencies suffered a major data breach at the hands of a nation-state threat actor who entered their systems via the company's third-party software. Both SolarWinds and Colonial Pipeline were private equity sponsor-owned or controlled portfolio companies. As CISOs in this space, what's keeping you up at night? Is generative AI making you sleep any less?

Bethany De Lude: Generative AI is making the hacker's toolkit more effective. You may no longer be able to rely on a familiar voice on the other end of the phone to verify who the caller really is. Executive impersonations are incredibly easy now because of this new technology. Using phishing as another example, you can't rely on poor grammar and other types of more obvious flags anymore. This technology has really added arrows to the hacker's quiver.

Key Takeaways

Private Equity CISO Fireside Chat: Cybersecurity Leadership in the Age of Generative AI

David Simon: When your teams are doing diligence on a potential deal, what does the review process look like for cyber issues? What is your level of engagement on these transactions as CISOs?

David Stern: My view on diligence is: Is the company capable of defending itself and dealing with an incident? If they don't have a secure organization, then the answer is no. If they have underfed security agency or IT organizations, then they're going to be a vulnerable target.

David Simon: Thank you both for sharing such valuable insights about what it means to be a CISO at this inflection point in the private equity space and beyond. From promoting robust cyber hygiene and awareness internally, to navigating a changing relationship with government cyber authorities, to leveraging new possibilities linked to generative AI all while mitigating the associated risks, there's undoubtedly plenty to keep CISOs busy today. Thank you both for your time!