Cyber in the Boardroom: Questions Every Director Should Ask Their CISO

Thought Leadership

Over the past decade, cybersecurity has been a frequent topic of conversation. Now, it has become a key agenda item for boards, with members responsible for overseeing and governing their company's cybersecurity posture. Government agencies have also stepped in, introducing several regulations such as requiring the detailing of risk management processes in annual reports.

Yet, despite increased governance efforts, cyberattacks are growing in velocity and intensity (companies disclosed around 9,500 attacks in the first half of 2024), and board member confidence in cybersecurity remains surprisingly low. In fact, a recent ***Harvard Business Review*** study found that 65% of board directors believe their organizations face a material cyberattack within the next 12 months, and nearly half feel unprepared for a targeted attack.

So, what are we missing? Where's the disconnect?

To bridge this gap, Korn Ferry spoke with a cross-section of Chief Information Security Officers (CISOs) from S&P 500 companies and privately held organizations to understand how to assess cyber preparedness.

Their insights helped inform our three-step strategy for:

- Making the most of discussions between board members and the CISO.
- Getting to the bottom line of what boards need to ask.
- Identifying what questions board members can ask their CISO to help close the gap.

STEP 1: TURN THE PAGE ON ATTACKS AND FOCUS ON RESILIENCE

Cyberattacks have become a real and persistent challenge for organizations. While board members may ask their CISO about the frequency and nature of these attacks, the more critical question is how well the company can recover when an attack occurs—because it's not a matter of "if," but "when" and "how."

As Justinian Fortenberry, former CISO and current Co-CTO at Etsy, points out, "[for] the companies that do best, it's often less about the breach itself and more about how they respond to the breach."

© 2025 Korn Ferry. All Rights Reserved.

While robust cybersecurity measures are critical, boards must shift their focus from preventing cyberattacks to building resilience—that is, their ability to anticipate, respond to, and recover from an incident. This starts with board members reorienting questions toward *cyber resilience*, which looks different for every company.

A current board member recalls that during her tenure as CISO at a Fortune 10 healthcare solutions provider, she made educating the board on the cybersecurity needs of IoT devices in their stores a key part of her security program. “Fraud is different [in retail pharmacies] than at a large diversified financial services organization,” she explains. Similarly, United Airlines CISO Deneen DeFiore emphasizes a cyber safety approach that addresses digital and systemic technology risks across the entire ecosystem. “Cybersecurity touches the whole portfolio of the business at United,” DeFiore says. “You can’t get a plane from point A to point B without hundreds of organizations and thousands of people interacting.”

What should CISOs and board members do to drive productive conversations on cyber resiliency? Jon Raper, CISO at Costco, suggests that the challenge is getting board members to dive into the true vulnerabilities. “You have to be overly transparent because you need to educate them on the [risks],” Raper says.

Sam Singer, Boeing's Chief Counsel for Cyber and Technology, emphasizes asking questions that get to the technology systems at the root of the issue, rather than focusing on metrics that often aren't probative of risk. "These abstract metrics have become the facts of cybersecurity, and that is the problem," he says.

Key Questions for the Boardroom

Board members should focus discussions on cyber resilience, not just attack prevention. Here are some questions to ask your CISO on this topic:

- How do we balance speed and efficiency with resilience?
- How does our technical debt impact the resilience of our company?
- How are we working to ensure that risk mitigation controls stay effective over time?
- How would our controls hold up to a malicious insider versus an unauthorized third party?
- How quickly are we doing vulnerability management? How fast can we go from detection to remediation?
- How long would it take to reboot after an incident?
- Are there any mission-critical areas where the organization should invest in resilience?

STEP 2: SHIFT THE NARRATIVE FROM COMPLIANCE TO RISK TOLERANCE

As cyber rules and regulations expand, board members naturally ask their CISO about compliance. However, compliance is just one aspect of cyber readiness. Instead, board members should focus on risk tolerance, recognizing that some level of risk is unavoidable and defining what the business can manage without jeopardizing its operations or goals. DeFiore, who is also a board member at Blackbaud, stresses that “strategy should ultimately be grounded in risk mitigation.”

As companies become more interconnected, even minor disruptions can have significant consequences. “There is no slack in the line anymore,” says Rob Nolan, CISO of Expeditors, a global logistics company, emphasizing the need for organizations to measure the financial impact of potential risks. Many of the CISOs we spoke with also stress the importance of not only *discussing* but also *quantifying* risk.

© 2025 Korn Ferry. All Rights Reserved.

We spoke with the CISO of a large dental insurer who noted that while qualitative assessments may have sufficed in the past, they are no longer enough. He suggested that in today's complex environment, the organization's risk profile and tolerance for variation must be expressed in a "quantitative" way. "This is not necessarily monetary, but some sort of a measurement system that we can all agree on that will help us understand how our risk profile is changing over time," he explains.

It's not enough to know that a risk exists; board members need to understand its potential financial impact to make informed decisions about where to invest in cybersecurity measures.

Key Questions for the Boardroom

Partnering with your CISO to define the organization's risk tolerance helps guarantee resilience, not just compliance. Here are key questions to ask your CISO:

- Do we have a clear understanding of our risk, and could this risk have a material impact if the organization is compromised?
- What are the highest priority risks that the organization needs to address?
- How do we plan to mitigate risks to our critical assets and business processes?
- What should the company's fault tolerance be?
- What incident response plans do we have in place, and how often are they tested?
- What metrics are we using to quantify our cybersecurity risks, and how are these metrics tracked over time?
- Can you provide examples of how we quantify the financial impact of specific cyber risks?

STEP 3: DON'T CUT THE MIC TOO EARLY

During board meetings, CISO may face the challenge of communicating highly complex issues in a limited time frame—sometimes as short as 15 minutes—impacting their ability to properly address critical concerns. As a board member, it's important to allocate enough time to thoroughly understand your organization's risks.

To make the most of your time *inside* the boardroom, consider organizing an executive session with your CISO *outside* of it. You may be surprised by the candor and insights that emerge without an official agenda. Or you may be encouraged by your CISO's willingness to engage and collaborate in a more open environment—free from the pressure of a ticking clock.

"To enable us to have those conversations, it's incredibly important to build that level of trust in informal settings," says Eric Hussey, CISO at Finastra. "It improves the environment so that if there is a problem, we can solve it together."

Spending time with your CISO in a less formal setting can help make future boardroom sessions more productive and engaging. Over time, this approach can boost confidence in the organization's cyber-readiness, bridging the divide between CISO practitioners and corporate governance leaders.

> "[For] the companies that do best, it's often **less about the breach itself** and **more about how they respond to the breach**.
>
> - Etsy Co-CTO Justinian Fortenberry

© 2025 Korn Ferry. All Rights Reserved.

Key Questions for the Boardroom

Engaging with your CISO informally can improve board sessions, strengthen cyber readiness, and close the gap between CISO and governance leaders. Here are some good questions to ask your CISO—*in* and *outside* the boardroom:

- What keeps you up at night when it comes to cybersecurity?
- What are the two things that are top of mind for you? What are you worried about most?
- What is the health or morale of your team?
- Do you have the resources that you need to protect the organization?
- What are the biggest challenges you face in implementing our cybersecurity measures?
- What support do you need from the Board to enhance our cybersecurity efforts?
- Do you have what you need to ensure our employees are aware of and trained in cybersecurity best practices?

HOW WE HELP

Korn Ferry partners with Board Members and Chief Information Security Officers to help them navigate the complexities of today's security environment. Our consultants specialize in delivering talent acquisition and advisory solutions that are tailored to meet the unique business challenges of the Boardroom and Cybersecurity organization.

Along with the questions supplied in this guide, here are additional questions to help board members tee up the conversation with their CISO during their next board meeting:

- What has changed in the company's risk landscape between now and the last time we spoke?
- Do we have a clear understanding of what our risk looks like today?
- What are the key risk indicators that we should be monitoring quarterly?
- How are these risk indicators changing and how do they relate to what is most critical to the business?
- What is cyber doing for the value of the company?

AUTHORS

Karena Man
Senior Client Partner
Technology & Digital Officers Practice
Korn Ferry

Natura De Pinto
Senior Associate
Technology & Digital Officers Practice
Korn Ferry

ABOUT KORN FERRY

Korn Ferry is a global organizational consulting firm, bringing together strategy and talent to drive superior performance for our clients. We work with clients to design their organizational structures, roles, and responsibilities. We help them hire the right people and advise them on how to reward, develop and motivate their workforce. And we help professionals navigate and advance their careers.

© 2025 Korn Ferry. All Rights Reserved.