McKinsey & Company

Risk & Resilience Practice

Competitive advantage through cybersecurity: A board-level perspective

Five leading cybersecurity executives and public company directors discuss how chief information security officers and boards can work together to grow and protect their organizations.

August 2025

The era when cybersecurity was a separate, isolated function at organizations is over. Today's threats, fueled by AI, require organizations to infuse "air to ground coverage"—from the boardroom down—across the institution. No one is more aware of these threats and the scale of the necessary response than an organization's chief information security officer (CISO).

At a recent panel discussion, McKinsey and the National Association of Corporate Directors (NACD) gathered five top CISOs and board directors to discuss how cybersecurity is changing, how organizations must shift their approach, and how CISOs and directors are uniquely positioned to co-lead the effort to keep institutions safe while benefiting from new technologies.

Moderated by McKinsey alumnus Justin Greis, the panel included Katie Jenkins, CISO at Liberty Mutual; Marco Maiurano, CISO at First Citizens Bank; Matt Rogers, independent director for Exelon; Noopur Davis, chief product and information security officer for Comcast and board member at Regions Bank and Entrust; and Nora Denzel, an NACD director, lead independent director at AMD, and a board member at Gen Digital and Sony Group.

This Q&A has been edited for clarity and length.

Justin Greis: Let's begin with the board's perspective. How do you think about cybersecurity? How do you approach the conversation?

Noopur Davis: What you cannot do is make it a discussion of technology in arcane terms that nobody understands. One way to approach it is through storytelling with data to back it up, and that seems to resonate. It forces us to simplify the message so the content is easy to understand in terms that stick in people's heads. Board members are typically very active and knowledgeable, so they will ask us pointed questions about our risks, and

Cybersecurity: A shared responsibility and a strategic edge

by Peter Gleason

Corporate boards and the C-suite used to think of cyber-risk management as an investment in avoiding loss—of data, money, and, importantly, trust. That view has evolved, and today cybersecurity is increasingly recognized as a driver of competitive advantage and critical-asset protection.

This shift is being accelerated by the rapid adoption of gen AI and by boards taking on more oversight responsibilities. At the center of this evolution is the chief information security officer (CISO), whose role has evolved from a technologist to a business partner—one who brings operational context to risk and positions the organization to adapt, not just react.

The panel discussion featured here—facilitated by the National Association of Corporate Directors (NACD) and McKinsey—is timely. The strength of the relationship between the board and the CISO is now a defining factor in long-term cyber resilience. Boards must build the fluency to align innovation, risk, and business strategies with what's ahead. And CISOs bring a level of expertise and context that the board likely does not have. While it can be difficult to achieve the right balance of give and take between the board and tech leadership, tech strategy and governance are at the heart of the board's and CISO's roles. Success, in the end, depends on seeing cybersecurity as both a shared responsibility and a strategic edge.

Thank you to McKinsey, the panelists, and everyone who participated in this important conversation. Let's keep this dialogue going.

Peter Gleason is president and CEO of NACD.

that gives us a chance to further drill down on their areas of interest (see sidebar, "The board and the CISO: Three questions to consider").

If the board asks you a question more than once, it should become part of your background materials. So our background materials are very detailed. There is a lot of data and a lot of detailed views of controls that can prompt further discussion. But the conversational bit is always more storytelling, and it works very well.

Katie Jenkins: If it's a stand-alone cyber briefing to a board committee, I'll start with the committee chair and ask, "Is there anything top of mind for you that you really want to hear about, that you haven't heard about in the past, or that's just bothering you?" That's important input; there are often topics or questions that are top of mind for directors, and getting those on the table at the very beginning allows us to identify them and decide to address them right away or put them in the parking lot for later.

I also catch clues from the hallway conversations before and after board meetings, which are so key because they often bubble up topics that should come up or give insight into where the real concerns are. I try to give my updates in person when possible because it creates a more open environment for discussion.

Marco Maiurano: The way I approach the topic of cybersecurity with the board is outside of the board meeting. I ask what they're hearing, what their concerns are, and what they've read that they want to understand. I also want to empower my board members to feel like they're armed with the necessary knowledge and answers to those questions so that they feel great coming into a

The board and the CISO: Three questions to consider

by Ida Kristensen

As we look across corporate boards, there's a lot of variation in how well the relationship between the board and the chief information security officer (CISO) works. Many boards are still on the journey to figure out the right oversight model when it comes to cybersecurity. Board members often express concerns about receiving too much material, not understanding technical jargon, and not knowing the right questions to ask, while the CISO may leave a board meeting feeling frustrated by a lack of alignment on priorities, budgets, and resources.

To ensure effective interactions, both the board and the CISO should consider three questions.

The 'why?': What each side perceives as the purpose of the board interaction matters greatly. If the CISO approaches the interaction as an uncomfortable exam or the board forgets it is "noses in, fingers out," the trust and quality of the conversation will suffer. In contrast, a joint mindset of "we are helping each other make our institution more secure" sets a much more constructive starting point for the discussion.

The 'what?': Understanding the "why" gives you direction for the "what." Board reporting is too often more about data than information. Conversations may focus too much on technology goals and capabilities and not enough on risks and threats. CISOs can be guilty of providing metrics that are easy to measure versus those that are of most interest to the board. All reports should relate to risks, risk appetite, and their implications for the organization.

The 'how?': The board's interaction with the CISO should extend beyond the scheduled time on the agenda. Ideally, there should be a broader set of interaction points and learning moments. Reflections from CISOs and board members alike highlight great practical examples of how to extend engagement beyond board meetings and build a more holistic relationship and shared journey.

The better the quality of conversations between CISOs and boards, the more secure our institutions and society will be.

Ida Kristensen is a senior partner in McKinsey's New York office.

meeting: "Hey, I've heard about these things. I now have some background. I can ask better questions." And that is really what the board is there to do—check, challenge, and oversee so we can collectively support the mission.

Matt Rogers: With energy infrastructure, cybersecurity is an ever-present risk. The industry does a great job in managing the risk, working with appropriate government agencies. In conversations with the CISO, step one is understanding what the threat profile is. This is the baseline conversation. If someone assumes the threat is not there, then they've likely already missed it. The second step is understanding where the risks lie. There should be an understanding of how to systematically close off those risks. The board's role is to ensure the company takes the risks off the table and, if there is an incident, ensuring that management and the board have a quick and disciplined response prepared.

Justin Greis: Nora, you often talk about the idea of air-to-ground coverage. Can you tell us a little bit about what that means to you from a governance standpoint?

Nora Denzel: You need air-to-ground coverage on technology because board composition varies. Most directors have financial acumen, but some board members may fall into the category of a "technology outsider"—someone who has limited experience with technology and may not have kept pace with today's emerging technology landscape. Then there are early adopters of technology and digital natives. CISOs need to be able to reach all types of directors, and often they find themselves in a messy middle.

In reality, CISOs are presenting to a bell curve of outsiders, technology immigrants [adopters who did not grow up using technology], and early adopters. And hopefully they'll get a digital native in there at some point. That's a diverse and challenging set of personas for any topic, let alone one as rapidly evolving and complex as cybersecurity.

NACD believes that a foundation of good governance is technology acumen, and we provide our members with trusted, independent research and thought leadership to help directors build their knowledge and apply true air-to-ground coverage. This is one reason NACD formed a 24-member Blue Ribbon Commission, publishing a report, *Technology Leadership in the Boardroom: Driving Trust and Value*, to help corporate boards navigate the fast pace of technology and innovation. We recommend that all boards have cybersecurity capabilities represented, just as we do in finance, so we can really drill down.

Marco Maiurano: My CEO asked me the same question of how I think about cyber. He observed, "The variability and severity are so drastic. Every day it's something different versus years ago, and any of those things has the potential to disrupt us."

That variability is where we need to make sure that we're educating the board, so they know how and where to dive down deep and make sure that we have that coverage top-down. We also have to let them know what we are doing about it and report in regularly on the key initiatives that are reducing risk and ensuring a resilient organization. Hopefully, those things reduce the severity and likelihood of the disruptions he mentioned.

We're doing education sessions and training. They have full access to me as well. I'll have lunch and learns with them, which is kind of fun. They'll pick a topic and say, "Hey, can we talk about this for a while?" If it's on their mind, we should talk about it. Forums like that give them the tools they need and provide choices in how far down they want to go.

One of the things that had them on high alert was the SEC [US Securities and Exchange Commission] guidance that had come out about the board being educated. We all took that very seriously, and everyone used it as an opportunity to learn and raise our collective game.

I am also seeing that our new members are coming in with backgrounds in some type of technology, and we are in the process of forming a new technology committee of the board. These new board members allow us to get more, and better-quality, airtime with the board, which I'm going to ultimately report on. That's how we're thinking

about getting that coverage, making sure the board is informed, and giving them the content and platform to ask the right questions.

Katie Jenkins: My job is not to overstate or underrepresent real risk; nothing good comes out of that. What I'm trying to impart is the way we're recognizing risk, qualifying and quantifying it, and mapping it to our initiatives to show the reduction in risk and hopefully accelerate real business value. Be it financial, strategic, or operational, my job is to accurately represent and balance value, cost, and risk.

One of the things I believe we do well is recognize the role of an independent assessment shared with the board as a good governance practice. At least annually, I take results from an independent global maturity assessment, using a consistent industry framework. While that framework may change over time, it provides an industry-standard, accurate, and complete representation of our maturity, which I can use as a comparison relative to our risk profile to determine if we are doing enough or if we need to step things up. If nothing else, our board can see a positive progression in our security posture as we make targeted efforts to improve it. There's also a benchmark so we can see where we sit within our peer group in our industry. While the assessment and benchmark are not a silver bullet in identifying all our issues, it at least helps provide a framework in which the board can think about our capabilities vis-à-vis our risks, and I can then have a conversation with the board on what we're doing about it.

Justin Greis: How do you think about governance and reporting for cybersecurity within a global and matrixed organization?

Noopur Davis: It's complicated, for sure. One of the boards I am on has a technology committee, and the other one has a cyber committee as a subcommittee of the audit committee. Those committees reflect the needs of the company. At Comcast, because it is so diversified and tech-centric, technology is a part of every conversation.

The way we govern is with representatives from Comcast's three big parts. There's the Comcast that everybody thinks about; there's NBCUniversal, which is news, entertainment, parks, and movie studios; and then there's Sky in Europe. Each organizational unit has a CISO who is responsible for cybersecurity and a corresponding board with oversight, because every one of those businesses has a unique—yet, in many ways, shared—risk profile.

Whenever we come together, we bring in all three of those constituencies. Each one talks about their particular risk and their area. Then we talk about common risks, such as AI, and what we are doing about it.

For example, when we talk about AI, we discuss what it means, opportunities and risks, and how it is being overseen in each company. Then we figure out the standards, policies, and guidelines that are common across all three. That works well. We have a high-level common layer of governance and a business-unit-specific layer, because as you can imagine, the risks to theme parks are very different from the risks to our broadband infrastructure.

Justin Greis: As a board, how do you all think about AI? And as board members, how do you govern it? And to the CISOs, how are you positioning AI from your seat?

Matt Rogers: AI is a great example of where risk shows up, how it shows up in new places, and the new faces who introduce those risks on a regular basis. It's the faces that are important. The CISO and the technology side can go only so far to protect the company, because the leaders on the front lines are the ones who are facing the risks directly and have the opportunity to mitigate any potential risks.

For example, you've got to spend time with the supply chain folks because suppliers can present a whole set of risks. You must spend time with the HR folks because companies now have people masquerading in online interview rooms. Boards have to empower managerial leadership across the company in a different way to ensure they are able to use technology while managing risk exposure.

It means ensuring leaders have the tools to protect the company and teaching them to be vigilant, because technology is only a tool. Management needs to be at the forefront of solving the problem.

AI is everywhere, and technology this pervasive raises questions about how companies and boards manage data, what we allow in, and what we do with AI. People are using AI in all kinds of different ways, and technology's not always going to catch the risks and keep them and organizations out of trouble. We need a whole set of leaders throughout the organization who provide the first line of defense. This is my example of air-to-ground coverage. You need people at the front line who really understand AI and can raise the right issue. Otherwise, we won't see it until it's too late. And you need people at the top who listen, understand, and take appropriate action based on the input of their teams. In this world, that's how you empower the front line; you need leaders who listen and act, especially since it may not show up as a technology issue.

Marco Maiurano: When I think about AI, and technology in general, it becomes the CISO's responsibility to figure it all out. What I've been doing with my board is articulating that it's not just about the CISO; it's about the data and what we want to do with it. It involves the chief data officer. It's about the second line of defense. It's about model risk management: how we're putting in governance and oversight. It's about the legal aspects, because there are things—especially in banking, a highly regulated sector—that can get us and our customers into a lot of trouble.

For AI, it's making sure that boards understand the opportunities that AI offers us and the pitfalls we need to avoid. I'm excited about AI but aware of the risks it introduces. As a first-line function, we can give the board confidence that we know how to manage it, we know how to govern it, we know how to identify where the risks are, and, most of all, we know how to identify what we don't know and where more work is needed.

Nora Denzel: NACD uses the term "technology governance" rather than "AI," because we know that tomorrow morning, somebody's going to come up with a new innovation that may introduce a whole new set of risks. We emphasize the importance of clarity on the board's role in governance, and after a board takes oversight action, it should update its charter to make it stick. Each of the committees has a different role, but technology oversight moves faster than any other I can think of.

The biggest risk you can take in the next five years is not taking on a technology risk. I've seen "nervous Nellies" on boards, including some who say, "Oh, we should tell the employees they are not to use ChatGPT." You can't go in with that. Leading boards go beyond compliance; they transition to strategic offense. These boards are considering the need for a technology or innovation committee to help the full board be proactive and get ahead of issues.

We're also telling boards to lean in and self-govern because technology is moving faster than regulation. Think back to when air bags were first introduced to make cars safer. Early air bag technology wasn't designed for women and children, and the result of that decision was disastrous. Regulation eventually made its way to the auto industry, bringing consumers the air bags we know today. This is a cautionary tale for boards who think being proactive on cyber and technology is simply nice to have.

Unfortunately, I don't think most boards are there. Sixteen percent of the Fortune 500 have technology committees now. I think it'll be well over 20 percent by the time proxy season is over. I'm not saying having a technology committee is the right thing, and it's certainly not a cure-all, but NACD tees this option up so boards can decide for themselves.

We also tell boards, "Focus on your data. Focus on your tech debt." No one ever wants to talk about this until there's a four-day outage, so we frequently communicate to boards that they need to self-govern and get educated.

CISOs and technology leaders can help boards improve their knowledge so they can stay ahead of technology opportunities and risks in meaningful ways. Most nominating and governance (nom-gov) committees include education in every board

meeting, and technology leaders should be working with that committee chair. However, boards know that management is also constantly learning and coming up to speed, so they will take a "trust then verify" approach to what they learn.

Noopur Davis: It depends on where the company is on its journey. For a company going through a technology transformation, the technology committee may focus on budgets, because they are investing hundreds of millions of dollars in business-changing transformation. As board members, we're asking: What is the tech debt? What is our plan of getting out? How do we adopt modern technologies? We're making sure that the company is thinking about it. But if you're on a technology committee in a company that's mature and they don't have a big new transformation, ask: "Why not?" Technology is disrupting so many industries that few are not looking at its impact and making the changes close behind.

Katie Jenkins is chief information security officer at Liberty Mutual. **Marco Maiurano** is CISO at First Citizens Bank. **Matt Rogers** is an independent director for Exelon. **Noopur Davis** is chief product and information security officer for Comcast and a board member at Regions Bank and Entrust. **Nora Denzel** is a director at the National Association of Corporate Directors (NACD), lead independent director at AMD, and a board member at Gen Digital and Sony Group. **Ida Kristensen** is a senior partner in McKinsey's New York office, and **Justin Greis** is an alumnus of the Chicago office.

McKinsey wishes to thank Peter Gleason, NACD president and CEO, and Marcel Bucsescu, NACD vice president of strategic engagement, for their collaboration and their contributions to the panel discussion.

Comments and opinions expressed by interviewees are their own and do not represent or reflect the opinions, policies, or positions of McKinsey & Company or have its endorsement.