McKinsey & Company

Risk & Resilience Practice

A board-level view of cyber resilience

The responsibilities of boards of directors regarding cybersecurity are changing significantly, as is the cybersecurity industry itself.

August 2024

Amid growing corporate and public sector cyber breaches and recent high-profile technology outages, significant changes are occurring both in the role of boards in cybersecurity and within the cybersecurity industry itself. In this interview, McKinsey's Sean Brown speaks with Vinnie Liu, the cofounder and CEO of the cybersecurity firm Bishop Fox, and McKinsey cyber-resilience experts Justin Greis and Daniel Wallance about how boards of directors should approach oversight of cybersecurity. The following is an edited transcript of their conversation.

For more discussions on the strategy issues that matter, follow the *Inside the Strategy Room* podcast on your preferred podcast platform.

Sean Brown: Boards' responsibilities are changing quickly in the face of emerging cybersecurity threats. Justin, tell us about your research on this subject.

Justin Greis: We set out to look at cybersecurity from two perspectives—that of the board and the cybersecurity community—to learn what they see as the core of the cybersecurity issues they face and how boards can arm themselves better.

As companies transform and modernize with more connected technologies, they increase their attack surface, which are the opportunities attackers can use to get into the company. Last year alone there was a 75 percent increase in intrusions into cloud-hosted environments, and that number is increasing, especially as companies move to the cloud more.

Vinnie Liu: When we observe how attackers work, oftentimes we see new technologies involved. They take advantage of these moments of technological change, such as migration to cloud storage, or the adoption of connected sensors within factories, or the adoption of gen AI [generative AI].These are moments of opportunity from an attacker's perspective. So when we think about the attack surface, it is not only what technologies you have but also what is changing in your company that we focus on.

Sean Brown: What are some of the biggest challenges that boards and their management teams face in the cybersecurity realm?

Justin Greis: A series of factors makes this topic complex for boards and management teams to digest. One is that the regulatory landscape is changing every day, with more and more countries—and industries—adopting new requirements around disclosure and privacy. There is also an increase in risk exposure as companies use more connected technologies. Also, it is extremely easy to launch cyberattacks. There is now a concept of ransomware as a service—it takes a few dollars and some effort, but it is relatively easy to launch these days.

Sean Brown: Take us through the board's specific responsibilities around cybersecurity and resilience. How are they evolving?

Justin Greis: One of the biggest things we talk about is making cybersecurity a competitive differentiator. This is a good question for all boards to ask as they assess their cybersecurity. How do they treat cyber? Is it a back-office function? Is it something viewed as a foundation of trust? If it is the latter, there is corresponding investment that goes along with that.

Another is the regulatory changes. For example, there are at least two in the US that are exceptionally important. One is CIRCIA: the Cyber Incident Reporting for Critical Infrastructure Act,[1] and another is the SEC [Securities and Exchange Commission] cyber-disclosure rule.[2] These have upended boards' obligations relative

[1] "Cyber Incident Reporting for Critical Infrastructure Act of 2022," CISA.gov, accessed August 2024.
[2] "SEC adopts rules on cybersecurity risk management, strategy, governance, and incident disclosure by public companies," US Securities and Exchange Commission press release, July 26, 2023.

> ‘When we think about the attack surface, it is not only what technologies you have but also what is changing in your company that we focus on.’
>
> —Vinnie Liu

to their knowledge of cybersecurity. Organizations need to be more conversant in cybersecurity in terms of their expertise, their training, and the designation of a cybersecurity expert on the board. It has to be somebody who asks good questions—and follow-up questions—and understands the preparation required and the investor scrutiny involved.

If you are a board member and you are seeing these regulations increase, and you are not getting sufficient answers to these questions, you have to keep asking until you understand the answers that you are getting.

Sean Brown: For those on the boards of global companies, how should they approach the cyber-regulatory landscape?

Justin Greis: First, you have to know the jurisdictions and the environments in which you are operating. You need to conduct a scan of the relevant regulations and laws that apply. The problem right now is that the disclosure requirements released by various governments have different timeframes for disclosure, what you need to disclose, to whom you need to disclose it, and the actions that you need to take as a result. There is a movement to try to harmonize regulations, but that is being done country by country. Globally, the requirements are still going to vary widely for the foreseeable future. Once you know what those requirements are, you need to get them into your response plans.

Sean Brown: Do you find that companies are prepared to meet those requirements and to rigorously defend against potential cyberattacks?

Justin Greis: Companies are struggling to invest in cybersecurity at pace with the changing threats and the rising threats. In our study of 114 companies, only 10 percent of them were what we call leading organizations starting to be able to protect themselves against advanced threats. The remaining 90 percent were below a level-three maturity, on a scale of zero to four.

That means most companies are not building capabilities that allow them to protect themselves. There are a number of reasons for that: underfunding, a lack of strategy, a lack of a

business-backed risk-based approach. In other words, the threats are moving faster than we can protect ourselves.

Sean Brown: What about state-sponsored attacks? It is hard for any one company to marshal enough resources to defend against such threats. Are companies and countries taking any collaborative approaches to this aspect of cybersecurity?

Justin Greis: There are public–private partnerships that are growing increasingly strong, and it is making a difference. Also, individual countries are developing national cybersecurity strategies to protect their virtual and digital borders. In the future, we are going to see stronger protections to protect against these nation-state attacks. For the short term, though, while a collaborative industry, everyone is still in the fight relatively alone, so companies have to protect themselves. Even when we have stronger state strategies and public–private partnerships, you will still have to lock your doors, so to speak. You still have to have good hygiene, protect the borders of your company, and do the things to keep you safe at night.

Vinnie Liu: One of the things to keep an eye on is the level of investment that governments are putting into areas such as sovereign-threat intelligence, and what they are doing to invest in their private sector organizations to defend them against attacks. It is not enough just to protect their own government networks. Public–private partnerships have become considerably better in the last few years. It is easier to collaborate before an incident, and oftentimes very difficult to collaborate during or right after one. You want to get ahead of attacks before they happen, and sharing intelligence is one way to do that.

Justin Greis: Another piece of the complexity here is that each organization takes a different approach to protecting itself. If you are a cybersecurity leader, you are probably thinking, "Well, I don't manage physical security, and I don't manage data privacy and protection. And somebody else handles backups." And that is the point. From a board standpoint, your obligation is to understand how well your organization handles cybersecurity and how you define your program irrespective of who has responsibilities for the individual capabilities. It may not be well understood who is doing what, even within the IT organization.

Sean Brown: Justin, what patterns are you seeing in the maturity levels of companies?

Justin Greis: We characterize cybersecurity maturity as two levels—foundational and advanced. In the beginning, 20 or 30 years ago, we saw many organizations that did not care. It just wasn't an issue for them. We do not see that as much these days. Today we challenge companies to develop a risk-based, business-backed view of cybersecurity. This means you prioritize and protect the things that matter most to your organization. Financial-services companies may be protecting financial and customer data, for example. Manufacturing organizations may prioritize availability of the manufacturing line. You have to understand first what the business is and then how to protect those business processes involved.

The next level of maturity is proactive security, where the cybersecurity function leads the way and can point out issues to the business and help the company move faster. This includes thinking in terms of security by design, where you embed security into the products' and systems' development processes so that security helps things go faster rather than slow things down.

> ‘From a board standpoint, your obligation is to understand [your organization’s cybersecurity capabilities] and how you define your program. . . . It may not be well understood who is doing what, even within the IT organization.’
>
> —Justin Greis

Sean Brown: Vinnie, what should boards understand about their organizations’ risk profile?

Vinnie Liu: Once we know where our assets are, we need to ask about the initial risk profile and what potential exploitation exists for these assets. This is an evolution and something you can take back to your organization and query your CISO [chief information security officer] about. Boards need to understand what their organizations are doing to get ahead of vulnerabilities before they are discovered and exploited by attackers.

And then we need to ask what we are doing to prepare to respond to or defend against attacks. Whether it is a tabletop exercise or an actual technical test—such as a red-team or penetration test to see our defensive behavior in action—what are the processes and human behaviors that will be involved in the response to an attack?

Attackers today are getting more creative. They are not always taking advantage of zero-day vulnerabilities, or vulnerabilities that have just been released, or rather, where a patch from the software vendor does not yet exist. More and more they are going into the back catalog of vulnerabilities and finding novel ways of taking advantage of them. They go after organizations that do not have consistent vulnerability management.

Sean Brown: What is the difference between the roles of the executive management team and the board?

Daniel Wallance: The responsibilities are separate, but we view them as a partnership. The executive team manages and runs cybersecurity in the organization, overseeing the people who deal with and mitigate risks daily. And they communicate the risks and status of threats and mitigating actions to the board and leadership.

And it is the board that needs to understand and ask questions about the maturity of the cybersecurity program, what risks are introduced, whether risk levels are within risk tolerance, and whether the risk tolerance levels are acceptable. Boards should not just ask questions. We also see boards actively engaging, for example, in tabletop exercises, in cyber simulations, to obtain an inside view of how the company's cybersecurity program is operating and what it means to defend and protect the organization.

Sean Brown: Justin, you have been studying boards' changing responsibilities around cybersecurity. What are the questions boards should ask?

Justin Greis: Board members as well as cybersecurity leaders and business leaders should ask: Can we clearly articulate what our risk tolerance is for cyber events? Do we have zero tolerance for downtime and disruption? Do we have limited or low tolerance for breaches that impact fewer than, for example, two hundred customers?

It is hard to decide how much you are willing to tolerate, but it is a really important exercise because the difference in cost, strategy, and focus between no tolerance and some tolerance or risk-adjusted tolerance is dramatic.

Boards will need to review their organizations' current and historical cyber-risk portfolio or register and confirm that decisions align to risk appetite. In a typical cyber-risk register, there are hundreds, if not thousands, of risks, and as many decisions that get made. For those risks that rise to the top, the questions to ask are, do boards know about them? How have these situations been decided, and are they in line with the risk appetite agreed to? Are cybersecurity leadership decisions in line with how the board would make decisions? Is the board comfortable with this?

Sean Brown: Talk more about resources and strategies boards should discuss with management.

Justin Greis: The first question we typically recommend asking is, what is our cybersecurity strategy, and do we have the appropriate resources to support it to decrease risk most effectively and efficiently? Often, we see that the CISO has been saying for years what is needed but the larger organization has not been able to understand what is being asked. Board members can help by assuming that their organization does not have the right allocation of resources and asking how they can help. They need to understand where additional cybersecurity budget should be spent if it were allocated.

Also, cybersecurity strategy is different from a cybersecurity operating model. And the capabilities that make up a cybersecurity organization vary from company to company. Boards need to understand "the what" (what needs to be done), "the how" (how to do so), "the who" (who needs to do the work), and the capabilities required to carry out the strategy.

Sean Brown: Do companies typically have to rebalance their technology investment to cover the resources needed for cybersecurity?

Justin Greis: In my experience working with companies on cost optimization and budget rebalancing, when they ask whether they can reduce their cybersecurity spend, the answer is almost always a "no," from a risk standpoint. When we dig in, we usually find the cybersecurity function

had been underresourced for years, which resulted in the need for increased spend to achieve sufficient risk reduction. Organizations should ask whether they are deploying resources in the most efficient and effective manner to decrease risk.

Sean Brown: What should boards be asking about third-party and fourth-party risks?

Justin Greis: Boards need to ask whether their organization tracks risks associated with vendors and third parties they use. We recently completed a study with the Institute of International Finance in which we asked top financial organizations' cybersecurity leaders where their organizations need improvement. By far, third-party cybersecurity risk or supply chain security management was the top capability that came up as needing improvement. We have seen a number of attacks involving critical third-party and fourth-party service providers that represent ecosystem risk to entire industries.

Whether your industry is healthcare or technology or financial services, understanding your third-party and fourth-party ecosystem and who drives those critical business processes, and what would happen if those vendors were to go down through a cyberattack or a natural disaster, is important.

Sean Brown: Does an organization need to prioritize identifying its assets to secure?

Vinnie Liu: This is a challenging problem because knowing where your assets are seems really straightforward, but it is a struggle we have seen for more than a decade within organizations. Board members would do well to refer to the Center for Internet Security's 18 Critical Security Controls, which offer a very straightforward way to understand the important controls to look for in an organization. This starts by asking the critical questions of: Where are my hardware assets? Where are my software assets? And where are my assets in general in an organization? It is critical to understand how to manage the security of the data elements. This is especially important today, as businesses become more digital in nature.

And then, you need to know not just where your IT assets are but where your operational assets or digitized factory assets are too. Those have become part of the expanded attack surface that Justin referred to. In more mature organizations, this is often someone's full-time job or part of a team whose job is to maintain an inventory of technology assets. And it is not enough to know what and where your assets are; you also need to be able to operationalize that data.

Sean Brown: Once you know those assets, how do you prioritize which ones to protect?

Vinnie Liu: I would suggest some thought exercises that can help your organization think this through. There is a concept that attackers go after vulnerabilities you have not identified, so you want to work to identify those weaknesses you are not yet aware of. This is why you want to know what your attack surface looks like.

Doing the opposite and looking at what you already know you want to protect is another type of valuable thought exercise. We often recommend that people look at their business continuity or disaster recovery plans, because you have already prioritized your most important assets there, and you can focus on securing them.

But here is the paradox—the assets that are the most important are often the ones that are the most connected to and critical in your operating model. They have the most paths in and out, which is where attackers will gain entry. Or they will find a

> ‘Understanding your third-party and fourth-party ecosystem and who drives those critical business processes, and what would happen if those vendors were to go down through a cyberattack or a natural disaster, is very important.’
>
> —Justin Greis

less important entry point that is less hardened and wind their way through the network to get through a trusted relationship to that critical asset.

When you think about your assets, you have to think about them and how you balance risk holistically. How you model your environment becomes critical. You have to find the paths that attackers will most likely take through your organization and layer these questions on top of one another to get to the point of answering the question, what do I need to do to protect it?

Sean Brown: Daniel, what expectations should boards have around cyber metrics and measurement?

Daniel Wallance: When we engage in the conversation around risk and capability maturity, the question becomes, what are the metrics we should be evaluating? The first point here is around risk, so the question to ask is about those assets that we just identified: What is the potential risk impact to those assets? For example, in the last 60 days, were there attempts to exfiltrate sensitive data such as customer repositories from the organization?

The second point is about maturity, and the questions to ask include: What is the state of our data protection controls? What is the state of our access management capabilities? What is the organization doing to enhance cybersecurity maturity to further decrease risk? And what is the progress toward improving and advancing our cybersecurity program?

Sean Brown: Adding to that, what types of metrics should companies and their boards watch to discern whether they are prepared?

Justin Greis: The problem with benchmarks is they have two fundamental flaws. First, the historical approach to cyber-resilience benchmarking is to think of cybersecurity spend in terms of percentage of IT budget. The problem with this is if you design your program to historical benchmarks, you are benchmarking to where programs were before, not where they are going given the threat landscape and the evolving cybersecurity capabilities. The second problem is that every organization is different, so trying to benchmark against others is comparing apples to oranges.

We suggest using benchmarks as one type of input that informs your strategy, rather than basing your strategy on benchmarks. Rather, design your strategy based on risk—use a bottom-up view of the capabilities you need to mitigate the risks you face.

Vinnie Liu: I cannot emphasize that point enough—every organization is different. I will give you an example: years ago, we were working with a very large and highly successful software company. But nobody could benchmark against them because of the investment they were making in cybersecurity. The moment we really understood that was when we learned that they had a person with the title "senior security ecosystem strategist." No other organization would have such a specific role.

The lesson here is that, as you are looking at your organization, be thoughtful about the differences between what you have heard or read in the news and the needs and capabilities of your specific company.

Sean Brown: Daniel, what should boards ask about incident management, so they understand how well their organizations have prepared to address an actual attack?

Daniel Wallance: The board should act as a challenge on the preparation and the ability of the organization to respond to cyberincidents, asking questions such as: Have we actually rehearsed these incident response plans? Are there incident retainers in place? Is there outside counsel available and noted to be called should a cyberattack happen? Will it be clear in the event of an incident who the incident commander will be in the organization? You do not want the CEO leading the day-to-day incident response. Would a nerve center be able to be stood up, and will it be clear who is participating? If we had to truly recover and rebuild our systems from backup or rebuild from scratch, would we be able to? We did a survey recently that found that only a minority of organizations are planning for such a recovery.

Also, we need to go beyond questionnaires and paper-based assessments and conduct hands-on keyboard exercises to know how effective the cybersecurity controls are. The board should understand whether systems will actually detect malware or block data from being exfiltrated. The board should seek to learn how effective the organization's cybersecurity capabilities would be in the event of a cybersecurity incident.

Vinnie Liu is a cofounder and the CEO of Bishop Fox. **Justin Greis** is a partner in McKinsey's Chicago office, **Daniel Wallance** is a senior expert in the New York office, and **Sean Brown** is a director of marketing and communications in the Boston office.

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.