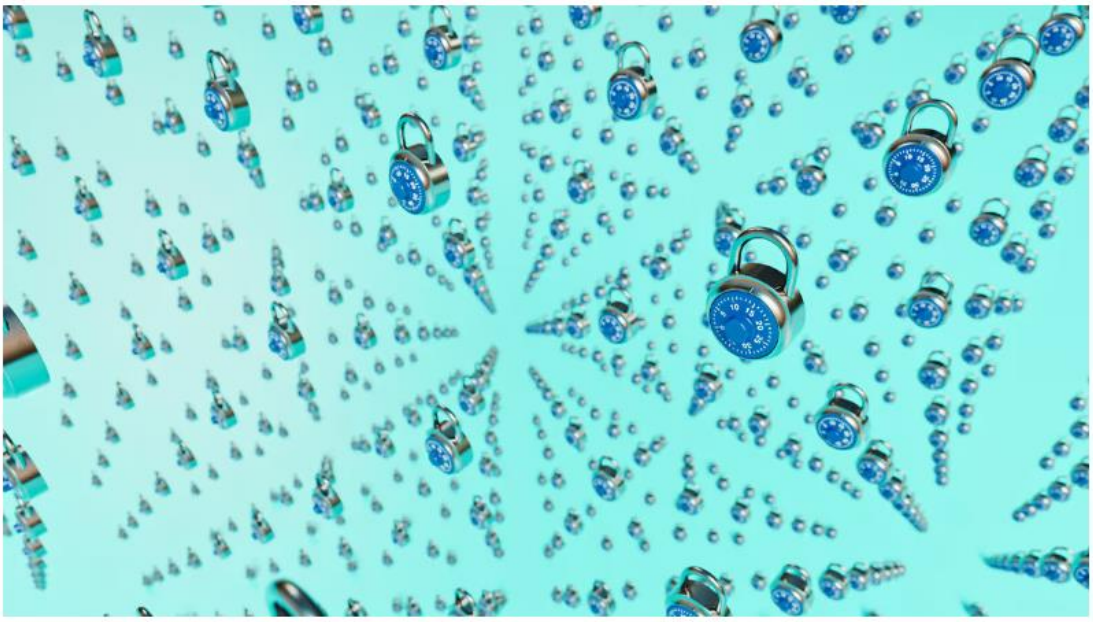
HARVARD BUSINESS REVIEW

Cybersecurity And Digital Privacy

Boards Are Falling Short on Cybersecurity

by Jeffrey Proudfoot and Stuart Madnick

April 2, 2026



Don Smith/Stocksy

At this point, most boards are convinced of the necessity for cybersecurity investments. They get that a serious cyber event is a costly, brand-damaging situation that can devastate operations, dismantle consumer confidence, and even conjure up existential concerns. However, as boards become more focused on cybersecurity, are they paradoxically getting worse at governing it? Year-over-year the cybersecurity situation keeps getting worse. For example, the 2024 FBI crime report, published last spring, revealed that cybercrime losses increased 33% compared to the previous year.

Based on our extensive program of board-focused research, including in-depth interviews with more than 75 directors and board-facing executives, we are concerned that despite boards placing greater emphasis on cyber risk, their ability to mitigate it has only marginally improved.

In our observations of board cyber governance, there are three prominent factors driving this problem: 1) there's a lack of cybersecurity expertise; 2) board-level conversations about AI ignore security; and 3) boards mistake regulatory compliance for security.

These problems are not insurmountable. But as long as they persist, boards are courting disaster. Here's what directors need to understand about their role in guiding cybersecurity efforts, and what they need to do differently.

The Lack of Cybersecurity Expertise

Many boards recognize that they're thin on cybersecurity expertise. A recent study found that out of 239 board members serving on cybersecurity committees spanning 62 firms, formal cybersecurity qualifications were uncommon: Only one director had formal cybersecurity education. Five had completed cybersecurity training or certifications, and just 16 contributed any relevant practical cybersecurity experience. Clearly, most board-level cybersecurity committees remain devoid of cybersecurity expertise.

Based on our conversations with directors, a common strategy for improving boards' cyber governance is emerging: adding cybersecurity-competent directors. On its face, it makes sense. Rather than trying to upskill the board to be more cyber savvy, simply adding one or two directors who already possess cyber knowledge seems like low-hanging fruit. As the numbers above suggest, most boards don't get beyond talking about it.

Yet even when boards succeed in recruiting cyber-savvy directors, the benefits may be constrained by the rapid pace of change in the cyber landscape. Reflecting on boards' difficulty staying current on cybersecurity, one director we spoke with observed:

> We don't have a lot of technologists that sit on boards. I sit on several boards. I'm the tech and cyber guy on all these boards. I'm not bashing my co-workers and co-board members. They're awesome people. But this stuff, AI and cyber, is moving so quickly. I have a hard time keeping up with it. And I know the technology, and I live in Silicon Valley.

What boards should do: In reality, the failure to bring in more directors with cybersecurity expertise may not be an oversight. From our interviews, correcting that weak point at the board level is the wrong use of time and effort. Rather than increasing the number of directors with cybersecurity expertise, boards

should concentrate their cybersecurity responsibilities on selecting and overseeing effective cybersecurity executives.

Instead of striving to become technical experts themselves, directors should focus on developing their ability to identify, evaluate, and recruit strong cybersecurity leadership and then provide effective governance of those leaders. Many directors are invited to serve on boards because of their successful executive experience, and this expertise can be leveraged and reframed to assess whether cybersecurity leaders are effective or ineffective. One way to make such an assessment is to observe executive performance in this context.

For example, although cyber incidents can be damaging and disruptive, they also offer an invaluable opportunity for boards to observe how executives respond under pressure. If cybersecurity leadership falls short during such crises and their ability to communicate effectively with the board is weak, it should prompt the board to consider leadership changes. In the absence of an actual breach, boards can similarly assess leadership capability through simulated cyber incident exercises or cyber fire drills.

To effectively adopt this redefined approach, directors should reassess how they engage with key executives about cyber. First, they should evaluate the clarity, relevance, and accessibility of security briefings. Second, they should get confirmation that the organization's cyber efforts and culture are focused on resilience and business continuity, rather than a narrow emphasis on implementing and testing technical controls. Third, they should consider the cadence of their interactions on cybersecurity, ensuring discussions are regular and strategic—not merely reactive to incidents or motivated by alarming headlines. Additionally, boards should bring in outside consultants to shore up their ability to provide proper cyber governance without becoming subject-matter-experts themselves.

AI is Both an Opportunity and a Risk

While artificial intelligence is a focal point of discussion in virtually every boardroom, these conversations are often myopic to strategy and all but ignore security. This tunnel vision on strategy is understandable enough. Boards are looking to AI for industry disruption, gains in operational efficiency, and the hope of developing novel products and services.

However, this strategic focus is the technological siren's song of our day, luring directors towards dangerous shores. AI is revolutionizing cybersecurity just as it's revolutionizing business: Malicious actors can now use it to streamline the generation of malware—harmful code that can attack your system—and increase the scale and speed of cyberattacks through automation. Further, AI can be used to create disconcertingly believable phishing emails (e.g., AI-supported spear phishing), as well as imagery, audio, and video for customized targeted attacks, which can lead to multimillion-dollar losses. Boards should be as alarmed about these AI-driven cybersecurity threats as they are enthusiastic about the business opportunities AI affords.

What boards should do: Boards must treat AI as both a strategic opportunity as well as a cybersecurity and governance risk. In practice, this means ensuring structured oversight of AI-driven threats, ethical implications, and operational vulnerabilities rather than focusing solely on its business potential. While AI's

positive capabilities often capture directors' attention, they must also consider how AI changes the organization's risk landscape—particularly how it may empower cyber attackers, introduce new vulnerabilities, and create ethical and operational challenges. (However, these efforts should align with the principles outlined in the previous section, with boards providing appropriate oversight of executives operating in this context).

Specifically, boards can ask questions like:

- Are we prioritizing the integration of AI because it creates actual value or because everyone else is doing it?
- Are we making compromising tradeoffs between AI adoption and AI risk that are unnecessary?
- How are our core processes changing due to AI and what are the implications if those processes are disrupted as a result?

Governance and ethics committees can play a central role by ensuring that AI risks are considered early in the design and deployment of AI tools and then integrated across board committees addressing technology, finance, people, and business impacts.

Because AI is already being integrated throughout many organizational contexts, boards should not delay in beginning to address it. Instead, they must engage now in providing meaningful oversight—understanding AI capabilities, articulating strategic objectives, and committing to the deployment of appropriate security guardrails—that will keep pace with the strategic efforts driving AI integration.

Compliance Isn't Security

The proliferation of cybersecurity regulations has lured many boards into thinking that compliance is the same as security. It's easy to see how this happens. Board discussions about cybersecurity regulations are time-intensive, as they often become mired in the details of dashboards, checking boxes, and ensuring that proper attestations of compliance are in order. But for the amount of board attention these tasks require, we have found that the connection between cyber regulations and good cybersecurity practices is tenuous, at best.

In reality, organizations large enough to have a board often get marginal value—if any—from cybersecurity regulations. Our investigations suggest that regulators are often poorly positioned to define cybersecurity "best practices," and that inherent bureaucratic processes create delays between regulatory development and implementation. As most organizations with a board have sufficient resources to hire top cyber talent, the regulations they are shackled with are often irrelevant and ill-timed.

When boards needed convincing that cybersecurity was important, regulations played a role in convincing them to sign off on cyber investments, but almost all boards have moved past that point. Speaking on this topic, one expert told us that regulations rarely add more than the already present threat of economic or reputational harm from a cyber incident:

I think the government has a hard time in this space getting past the mindset of "go to the battle and shoot the wounded" [i.e., punishing companies that have experienced a cyber incident]. … And if you view shooting the wounded as a useful exercise in morale boosting, then that tells you all you need to know about cybersecurity regulations.

What boards should do: Boards should view cybersecurity less as a compliance-driven regulatory issue and more as a competitive, operational resilience issue, where market incentives and organizational accountability drive stronger security outcomes than government-imposed rules. The dynamic is closer to airline safety than traditional regulation, where organizations are motivated to improve because the consequences of failure—such as operational disruption, financial loss, and reputational damage—are immediate and severe.

As a result, boards should emphasize internal incentives, accountability, and operational discipline, treating cybersecurity as a core component of resilience and long-term competitiveness. To ensure that boards are aligned with this new perspective, they should consider questions like:

- To what extent are cyber elements integrated into the development of our products and services?
- Is the board addressing cyber in a proactive or reactive manner?
- How can improved cybersecurity improve customer experiences and brand reputation.

Furthermore, the board needs to realize cybersecurity risks often extend beyond the boundaries of a single organization, as vulnerabilities can exist across interconnected systems and sectors with dramatic consequences. Since risk oversight is one of the most important jobs for the board, these risks must be carefully studied.

To address extraorganizational risk, boards should ensure that executives treat this category as a strategic priority. They should actively probe to identify high-risk partners, confirm that external threats are fully integrated into business continuity plans, and verify that appropriate redundancies exist for critical functions. Equally important, boards should encourage partners to adopt a more advanced posture—shifting away from viewing compliance as synonymous with security and toward recognizing it as a driver of resilience and competitive advantage.

. . .

It is encouraging that more and more boards realize that they have an important role to play in overseeing the fiduciary and risk oversight responsibilities related to cybersecurity. But many do not yet understand exactly how to most effectively accomplish that role. Directors need to consider the three key shortcomings above and how they might address them.

In response, boards should recognize that their most effective lever is not trying to add technical expertise at the board level or relying on training that quickly becomes outdated in an AI-driven threat environment.

Instead, they should focus on having the highest quality cybersecurity leadership and empowering them to maximize their impact.

By treating regulatory compliance as a baseline requirement—rather than a substitute for strong cybersecurity practices—boards can work with management to strengthen the organization's security posture for sound strategic reasons, such as protecting the brand or enabling product differentiation.

With these shifts, boards can engage more productively with executives to ensure that AI-enabled business strategies do not create blind spots in identifying and responding to an equally fast-evolving, AI-driven threat landscape.

Acknowledgement: The research reported in this article was supported, in part, by funds from the members of the Cybersecurity at MIT Sloan (CAMS) consortium.

Jeffrey Proudfoot is a professor in the Computer Information Systems department at Bentley University and a Cybersecurity at MIT Sloan (CAMS) research affiliate in the Sloan School of Management. His research focuses on organizational cybersecurity topics, including regulations, compliance, executive leadership and board governance.

Stuart Madnick is the John Norris Maguire Professor of Information Technologies in the MIT Sloan School of Management, Professor of Engineering Systems in the MIT School of Engineering, and Director of Cybersecurity at MIT Sloan (CAMS). He has been active in the cybersecurity field since co-authoring the book *Computer Security* in 1979.