Harvard
Business
Review

IT Management

Boards Are Having the Wrong Conversations About Cybersecurity

by Lucia Milică and Dr. Keri Pearlson

May 02, 2023

Helen King/Getty Images

Summary. Headlines increasingly highlight the consequences of poor cybersecurity practices. Board members with cybersecurity experience are trying to get their fellow members' attention on it. And board members want to provide oversight, even though they just don't have the right questions to ask. Boards need to discuss their organization's cybersecurity-induced risks and evaluate plans to

manage those risks. With the right conversations about keeping the company resilient, they can take the next step to provide adequate cybersecurity oversight.

close

Boards that struggle with their role in providing oversight for cybersecurity create a security problem for their organizations. Even though boards say cybersecurity is a priority, they have a long way to go to help their organizations become resilient to cyberattacks. And by not focusing on resilience, boards fail their companies.

We surveyed 600 board members about their attitudes and activities around cybersecurity. Our research shows that despite investments of time and money, most directors (65%) still believe their organizations are at risk of a material cyberattack within the next 12 months, and almost half believe they are unprepared to cope with a targeted attack. Unfortunately, this growing awareness of cyber risk is not driving better preparedness. In this article we detail several ways companies can begin to develop better cybersecurity awareness.

Board interactions with the CISO are lacking

Just 69% of responding board members see eye-to-eye with their chief information security officers (CISOs). Fewer than half (47%) of members serve on boards that interact with their CISOs regularly, and almost a third of them only see their CISOs at board presentations. This means that directors and security leaders spend far from enough time together to have a meaningful dialogue about cybersecurity priorities and strategies. In addition, our research found that while 65% of board members think their organization is at risk of a material cyberattack, only 48% of CISOs share that view. This communication gap and board-CISO misalignment hinders progress in cybersecurity.

Our findings suggest that the CISO-board disconnect is exacerbated by their unfamiliarity with each other on a personal level (they do not spend enough time together to get to know each other and their attitudes and priorities in a productive way). Also contributing to this disconnect is the CISO's difficulty in translating technical jargon into business language, such as risk, reputation, and resilience.

To forge strategic partnerships with CISOs, director-CISO engagement between board meetings would enable directors to ask better questions and understand the answers they receive.

Boards focus on protection when they need to focus on resilience

Notwithstanding the high perceived risk, our survey found that 76% of board members believe they have made adequate investments in cyber protection. Furthermore, 87% expect their cybersecurity budgets to grow in the next 12 months.

However, their investments may not be in the right areas. In a typical board meeting, the cybersecurity presentations usually cover threats and the actions/technologies the company is implementing to protect against them. For example, in many board meetings, the primary topic is how often the company administers a phishing test and the statistical results. To us, that is the wrong perspective for board oversight. We know we cannot be completely protected, no matter how much money we invest in technologies or programs to stop cyberattacks. While spending resources to protect our assets is critical, limiting discussions to protection sets us up for disaster.

Instead, the conversation needs to focus on resilience. We must assume, for planning purposes, that we will experience a cyberattack of some type, and prepare our organizations to respond and recover with minimal damage, cost, and reputational

impact. For example, instead of going into detail in a board meeting on how our organization is set up to respond to an incident, we must focus on what the biggest risk might be and how we are prepared to quickly recover from the damage should that situation happen.

To change their focus to resilience as the primary goal of cybersecurity, directors could ask their operating leaders to create a vision for how the company will respond and recover when an attack occurs. Minimization of the possibility of a successful cyberattack in the first place should only be the secondary goal.

Boards view cybersecurity as a technical topic, but it has become an organizational and strategic imperative

Only 67% of board members believe human error is their biggest cyber vulnerability, although findings of the World Economic Forum indicate that human error accounts for 95% of cybersecurity incidents. This might be an indicator that some boards do not see the organizational risk they face. Further, half of survey participants value CISO cybersecurity expertise the most, followed by technical expertise (44%) and risk management (38%). This suggests that even though cybersecurity topics may have made it onto the agenda, the board still sees them as technical issues.

When boards view cybersecurity only as a technical topic, it becomes a topic too operational for attention in their meetings. Time is limited in board meetings, making it difficult to cover all the nuances necessary for proper oversight. Directors may shy away from asking difficult questions because they feel they are not knowledgeable enough about technical concepts to properly articulate the question or even to understand the answer. Viewing cybersecurity as an organizational issue changes the discussion

from a technical to a management challenge. When cybersecurity is viewed as an organizational strategic imperative, it becomes relevant for board level discussion.

Boards should ask questions such as, “What is the technical risk to our business from potential cybersecurity incidents?” “What are we doing about tempering any damage resulting from the realization of that risk?” “What is the organizational risk from potential cyber incidents and what are we doing to quickly recover from the consequences?” And, “What is the supply chain risk from potential cybersecurity incidents and what are we doing about it so we do not lose a day of production?”

The composition of most boards today creates additional vulnerability when it could create stronger oversight

Many boards we studied are composed of very seasoned executives, either retired or not, who have extensive experience in operations, finance, sales, and their industries. But few have cybersecurity knowledge or experience. In 2022, the SEC proposed more explicit recommendations for cybersecurity risk management, governance, and disclosure for public companies, and it’s expected that these proposals will become requirements. That means that boards must have clearer oversight of cybersecurity risk and include explicit cybersecurity expertise on the board.

Many former executives were leaders before the current cybersecurity environment, and may not bring expertise, or even an approach for gaining that expertise, to their boards. Not that they are inappropriate executives to serve as directors without such expertise, but the board must develop this expertise as a whole. Directors must bring more than just technical expertise to the boardroom. They must also understand the environment,

financial structures, tradeoffs, and business risk portfolio. Finding new board members who bring the right mix of cybersecurity expertise and business acumen is challenging.

To bring cybersecurity expertise into the boardroom, board composition may need to change. Board members may need to gain cybersecurity expertise through frequent conversations about cybersecurity-generated risk, training, and development programs, and add colleagues with radically different business and professional backgrounds than current board members.

Failing to show that cybersecurity is a priority for the board sends an unwanted message

Our research found that almost a quarter of boardrooms do not view cybersecurity as a priority, and many do not even regularly discuss the topic. Some boards only have one cybersecurity update presentation per year, and that presentation is usually focused on how protected the organization is. That is not adequate.

Making cybersecurity a priority for the board is a commitment, not merely an annual update. It means talking about it at every board meeting, getting updates in between meetings, asking questions outside of what is presented, and taking a personal interest (such as being secure themselves, bringing cyber questions up and/or sharing stories, making heroes out of those who show the behaviors that the board wants to see, etc.).

For example, what message would be sent to the organization's executive leadership if, at each board meeting the members recognized an exemplary "hero" who had personally done something to increase the resilience/security of the company? On the other side, if the board does not up their game by showing how important cybersecurity is to them, intentionally or not, they are communicating that cyber is not a priority.

Directors' personal actions send messages to the senior leaders. By making cybersecurity a personal priority through actions and investment of time and attention, directors show how important it is.

Boards know they must do something different. The SEC recommendations would codify that knowledge. Headlines increasingly highlight the consequences of poor cybersecurity practices. Board members with cybersecurity experience are trying to get their fellow members' attention on it. And board members want to provide oversight, even though they just don't have the right questions to ask. Boards need to discuss their organization's cybersecurity-induced risks and evaluate plans to manage those risks. With the right conversations about keeping the company resilient, they can take the next step to provide adequate cybersecurity oversight.

LM

Lucia Milică is Global Resident CISO at Proofpoint.

DP

Dr. Keri Pearlson is the Executive Director of the research consortium Cybersecurity at MIT Sloan (CAMS). Her research investigates organizational, strategic, management, and leadership issues in cybersecurity. Her current focus is on the board's role in cybersecurity.