Cybersecurity at MIT Sloan

Harvard Business Review

Keri Pearlson

October 4, 2023

A Tool to Help Boards Measure Cyber Resilience

____

By now most boards know that cybersecurity is a business risk that they must oversee and ensure proper mitigations are in place. In an earlier article, we described the conversations the boards must have to perform this role. We made a case for discussing cyber resilience instead of cyber protection. Organizations cannot protect themselves enough to simply rely on additional investments in protection. Certainly, protecting assets, systems, and data is critically important, but as continued headlines have shown, focusing on protection is just not enough. Companies, and the boards that oversee them, have failed to find the right way to be protected enough (as evidenced by the constant headlines sharing the latest innovative breach on the under protected organization). Instead, we advocate that boards must have conversations about resilience, not just about protection.

To properly mitigate cyber risk, company leaders must have rock-solid plans in place to respond and recover quickly so even in the face of a cyber attack, the company continues to operate. Those are the right conversations for board directors to have with their cybersecurity leaders. In this article, we share research on the kind of information directors need for these conversations, and it is not the information they are getting today.

Research into Board Oversight

The board provides oversight to operational and strategic decisions and has a fiduciary responsibility to manage cyber risk. We began our research by trying to understand the kind of information CISOs and cyber executives were reporting to their boards, and comparing it to the information boards need to do their job. We set up a survey with many different kinds of performance indicators, ranging from technical to organizational. But the results of that survey made it clear that we were on the wrong path.

While it's easiest for cyber executives to report on technology metrics or organizational metrics, such as phishing exercise results, this information does not help the Board with their job of ensuring cyber resilience. It's just the wrong level of information. It's important for operational cyber leaders to understand how their security controls are set up, how they are functioning, and where they are failing. That's the operational leader's job. But it's the wrong information — at least initially — for conversations with the board.

We changed direction and applied the concept of a balanced scorecard (created by Harvard professors Bob Kaplan and David Norton) to cybersecurity. We asked questions of cyber leaders who report to boards, board members, and other subject matter experts about the information most useful to boards from a business perspective, rather than a technical perspective. This approach yielded a framework and set of recommendations that hold promise to assist boards in understanding the real risks they face, give cyber executives a language to communicate these risks, and create opportunity for useful dialogue between the two groups.

The Need For Better Board Cybersecurity Reporting

...

____

TO CONTINUE, SCAN QR CODE

____

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.*

____

THIS QR CODE WILL DIRECT YOU TO THE CAMS WEBSITE
https://cams.mit.edu
SCAN ME

THIS QR CODE WILL GIVE YOU ACCESS TO A DIGITAL COPY OF THE ARTICLE
SCAN ME