Harvard
Business
Review

Cybersecurity and Digital Privacy

A Tool to Help Boards Measure Cyber Resilience

by Dr. Keri Pearlson

October 04, 2023

Helen King/Getty Busà Photography/Getty Images

Summary. During our research, we asked cybersecurity leaders, board directors and other subject matter experts about board cybersecurity discussions and the reporting given to boards in preparation for these discussions. All respondents had strong opinions about cybersecurity boardroom discussions. Generally, participants agreed that boards had a

difficult time discussing cybersecurity at a meaningful level, the board needed different information, and a new approach was necessary.

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

During our research, we asked cybersecurity leaders, board directors and other subject matter experts about board cybersecurity discussions and the reporting given to boards in preparation for these discussions. All respondents had strong opinions about cybersecurity boardroom discussions. Generally, participants agreed that boards had a difficult time discussing cybersecurity at

a meaningful level, the board needed different information, and a new approach was necessary. For example, one director responded said, “I think a discussion about cybersecurity metrics is worthwhile. It’s hard to measure and communicate security ‘value.’ So, some thoughts in that regard would be interesting to me.”

But cybersecurity was not even a board level topic for some respondents. One of the respondents commented, “None of the Boards on which I’m serving have a specific focus on cybersecurity. For one board, it’s included in the IT topics we discuss. In another, it’s part of the audit committee.”

One respondent who identified as a C-level technical leader observed that boards want comparisons, especially for making assessments about cyber resilience. He said, “My board is interested in resilience, but also curious about what others are doing. They value peer insights and comparisons.”

Participants wanted key information about system assets, proactive capabilities and how quickly they could recover when asked what information would help them to assess operational risk. One of them was a board member of a technology services identified the information he would like to know, “What date types we have, where we have them, likelihood of compromise to their confidentiality, integrity, availability, and impact of their security’s compromise to our business operations.”

More than half of the participants wanted to know the financial dollar value involved with breaches or cyber-attacks on their organization. Almost half of the participants mentioned the use of third-party technical risk assessments, which they reported to the board and updated every quarter. For the supply-chain, respondents thought it was important to know about capabilities and

protection of suppliers and redundant options. However, most of the respondents were not sure if technical and supply-chain details should be part of the oversight for the board.

There were mixed responses when asked about what they thought would help access organizational risk due to cybersecurity vulnerabilities. Some respondents were not sure what would be needed for them to assess organizational risk. Some mentioned reviewing training details, others commented that an assessment of employees' skills to handle potential organizational vulnerabilities.

Interviews revealed that boards frequently delegate responsibility of cybersecurity to audit and risk committees. Respondents commented that feedback from these committees was welcome when the board receives cybersecurity reports.

Resilience assessment was also explored. Half of the respondents did not have a method for assessing overall organizational resilience to cybersecurity risks. Respondents commented that financial, supply-chain, technological and organizational risk assessment might lead them draw inferences to overall organizational resilience, but it was the role of operational leaders to present these risks to the board and to have a plan in place to address these risks.

Follow up discussions with respondents made it clear that board members were interested in making sure their organizations were resilient to cyber risks, and that there was a lack of tools to help boards perform appropriate cybersecurity oversight for these concerns.

The Balanced Scorecard for Cyber Resilience (BSCR)

Building on the original Kaplan and Norton work, a balanced scorecard incorporates important performance indicators from different perspectives of the company that provide leaders with complex information that is easily understood. The main purpose of their scorecard was to provide insight into financial and operational performance by combining information about core activities that might otherwise be isolated from each other. By looking at these indicators together in a single framework, the leaders are able to draw conclusions that might otherwise be missed. Our work extended these ideas into the cybersecurity realm to provide insight to boards about cyber resilience.

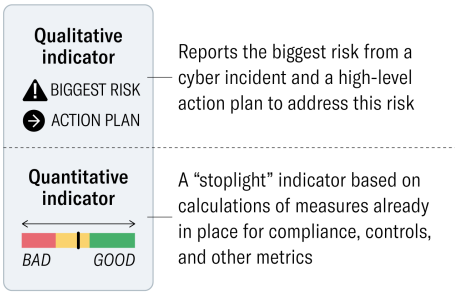
The board level balanced scorecard for cyber resilience is shown in Figure 1. It combines financial, technological, organizational, and supply-chain indicators, and an aggregated indicator of resilience. Each of the four quadrants has three components: 1) the biggest risk, 2) the action plan for managing that risk, and 3) an overall indicator (green, yellow, or red) for quick assessment of risk to that area. These four quadrants are based on findings from current research but leave open the possibility of additional areas that might be relevant to assessing cyber resilience in the future.

Figure 1: Sample of a board level Balanced Scorecard for Cyber Resilience (BSCR) for an organization

A Balanced Scorecard for Cyber Resilience

The balanced scorecard for cyber resilience (BSCR) includes four quadrants, each one reporting assessments of cyber risk for key aspects of the business. In each quadrant there is a qualitative and quantitative component. The qualitative component is a short description of the risk most concerning to the operational leaders, and the quantitative component is an indicator of how well cybersecurity activities meet expectations based on metrics set by management.

Components of a cyber-resilience assessment:



Sample scorecard:

Source: Keri Pearlson

HBR

See more HBR charts in Data & Visuals

Components of the Board Level BSCR

Each quadrant of the board level BSCR is designed to provide directors with business relevant indicators of the strength of resilience and the biggest risk from that area.

- The Stoplight indicator is a quickly understood indicator of a quantitative assessment of key components of cyber risk. This is compiled from operational data cyber leaders use to manage cyber activities. These indicators might come from frameworks such as the CISA Cybersecurity Performance Goals (CPG) or home-developed metrics used by the cybersecurity team to monitor activity.

- The Biggest Risk window is a qualitative assessment made by knowledgeable cybersecurity leaders, such as the CISO or CIO, of the most problematic issue in that area. It's a brief answer to the questions, "what is the biggest risk the organization faces right now?" and "how big is this risk?"

- The Action Plan is the leader's high-level plan to manage the biggest risk. It is the answer to the questions "What are we doing about this risk right now?" and "How urgent is this risk?"

This board level BSCR provides directors with quickly understandable information based on both qualitative, managerial insights and quantitative cumulative data to spark deeper conversations with operational managers.

Providing The Right Information to Boards

Directors understand their organization faces risk from many sources, including cybersecurity risk. The big elephant in the room, however, is how to appropriately discuss and manage this risk. Cybersecurity executives know that their organization cannot be 100% secure, since new threat vectors emerge regularly, and new vulnerabilities are uncovered at a similar rate. Managing the risk means making decisions on the best way to spend resources protecting our organization and at the same time, preparing for a possible incident and insuring resilience to operations. For this, boards need a balanced view of cyber vulnerabilities and threats and an understanding of how operational leaders are managing them.

While it is seductive for directors and operational leaders to focus on the technical details and metrics, it's not the right place to start. For example, when cybersecurity leaders only report the latest phishing exercise results, boards engage at that level. Quantitate measures are easy to obtain, share, and compare. But they don't tell the story that help boards oversee cybersecurity risk. Further, directors use the information they are given, and the ensuing discussion focuses on tactical plans operational leaders put in place to reduce the chance of a successful phishing email. But that is not the best use of the directors' attention. It focuses the directors' attention on one aspect of organizational cybersecurity and may miss other vulnerabilities that threaten the business. Instead, the board should be discussing the business-level risks the leaders see, and what the operational leaders are doing to insure resiliency. This broader question leaves open the opportunity for any organizational vulnerability, not just a phishing email vulnerability.

What Are the Next Steps?

From our work, we see that a change in mindset from protection to resilience is needed and to drive that change, operational leaders must change how they report to the board.

Managers focus on measures taken for cyber protection, but boards need to know about cyber resilience. Managers think their boards want to know about operational metrics, but directors really want to know the business risks the managers anticipate and what action plan is in place to mitigate the risk.

Managers report on metrics they can calculate, but boards need a broader assessment of where the next cyber issue might occur and those might not be quantifiable. Directors need information about the business impact of the cyber risks, both from a risk-identification and a risk-likelihood perspective. Qualitatively reporting the general business risks from cyber threats and vulnerabilities in the context of how it might disrupt the organization, and discussing the importance of the risk with the board enables directors to assess if attention is placed on the right risks and mitigation strategies.

The value of discussing a balanced view of cybersecurity risks at the board level does not come from comparing today's posture with yesterday's posture, but from making sure that the business is prepared today and tomorrow for potential disruption from a cyber incident. Cyber risk is dynamic. What is a risk today may not be a risk tomorrow, or it might be the biggest risk tomorrow. To make that assessment, boards want to have the right conversations with those who know both the cyber risk and the business impact of that risk.

It’s not really about how protected we are, but how resilient we are. A Balanced Scorecard for Cyber Resilience is the starting place for the discussions about how the business will continue operations when an event occurs. It is not enough to invest only in protection today. We need to focus on business resilience to cyber vulnerabilities and threats. To do that, we need a balanced, qualitative assessment from the operational leaders who know.

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.