Board Level Balanced Scorecard for Cyber Resilience

Dr. Keri Pearlson
Cybersecurity at MIT Sloan, MIT
kerip@mit.edu

Mridula Prakash
Cybersecurity at MIT Sloan, MIT
mridula@mit.edu

Abstract

Boards of Directors (BODs) have a unique role in managing cybersecurity: they provide oversight to operational and strategic decisions while executing a fiduciary responsibility to manage cyber-risk. Since organizations cannot count on 100% protection, BODs must ensure their organizations are cyber-resilient, and can recover quickly from cyber incidents. But BOD reporting mechanisms are inadequate for this role. Most of the reporting to BODs are on operational metrics around protection, not cyber-resilience and the business at risk from a cyber incident.

This paper suggests a balanced scorecard for cyber resilience (BSCR) for BODs. This theory-building research was informed by surveys and focus groups of cybersecurity leaders and board members. The BSCR gives business context-based insights and metrics on the biggest risks to cybersecurity resilience faced by their organization, and the investments their operational managers have made to mitigate the impact of these risks. Armed with the BSCR, BODs have the information they need for meaningful discussions and evaluation of their organization's cyber-resiliency.

Keywords: cybersecurity, cyber resilience, boards of directors, balanced scorecard, cyber risk.

1. Introduction

Boards of Directors (BOD) provide oversight to operational and strategic decisions and insure fiduciary responsibility (Milică & Pearlson, 2023). They must make sure operational managers have made the best decisions possible to reduce risk and ensure business resilience (Coden et al., 2022). Among other things, boards are accountable for oversight of business activities and strategies that guide revenue and spending. They must ensure regulatory compliance and manage risk (Milică & Pearlson, 2023). In today's business environment, acceleration of cyber security risk has raised the concern for many boards (Deloitte, 2021). Cyber breaches translate into business losses, adversely affecting stock prices and companies' valuation hampering the shareholders' wealth (Tosun, 2021). Further, the accelerated digitization of businesses and the use of new technologies such as AI and hybrid cloud have brought cybersecurity concerns to the forefront of risks to be managed by boards. Boards need the right information to understand and manage cyber risk. They need a balanced scorecard of the different risks to their organization's cyber resilience.

Board members are experts in understanding risk and risk management since this is part of their regular oversight and fiduciary responsibility. Directors are often experts at managing financial risk, business risk, and organizational risk. However, managing cyber risk requires the board to have specialized experience and different information than other risks. Cyber risk is a dynamic view of vulnerabilities an organization faces as the result of malicious actors' intent on stealing assets or disrupting operations (Zeijlemaker et al., 2022). Since the threats change regularly, cyber expertise helps a board understand the risks faced and the questions to ask to dive deeper into explanations and alternatives. But the information needed to understand the cybersecurity opportunities and threats is different than the information necessary to understand other business risks. Evaluation of expenses and revenues is not going to highlight where the cyber risk impacts the business, and understanding information systems and technical performance indicators are not going to highlight how resilient the business is to a cyber incident. The research provides new ways to discuss cyber risk at the BOD level.

This paper presents a solution to this challenge by creating a board level balanced scorecard for cyber resilience (BSCR). Building on the classic "balanced scorecard" developed by Kaplan and Norton (Kaplan & Norton, 1992) the BSCR is based on the premise that cybersecurity is a complex problem that cannot be solved by technology alone. The BSCR is designed to combine dimensions that impact cybersecurity-organizational, financial, supply-chain, and technology (Pearlson et al.,2020).

The BSCR has three layers of detail that are useful to different levels of management and leadership of an

URI: https://hdl.handle.net/10125/107196
978-0-9981331-7-1
(CC BY-NC-ND 4.0)

organization. Support for the information reported in the board level BSCR comes from operational KPIs. To represent that information, this work maps measures from the Cyber Performance Goals (CPG) framework created by the Cybersecurity Infrastructure Security Agency (CISA) (Cybersecurity Infastructure & Security Agency, 2021). The BSCR is a tool to provide understanding of cyber risk impacts, to link risk to operational KPIs, and to spark discussion about what can be done to manage ensuing cyber risk.

After a brief overview of relevant background literature and research methods, this paper describes the BSCR, maps the indicators to the CISA Cybersecurity Performance Goals (CPG) (Cybersecurity Performance Goals, 2021) and discusses uses and limitations of the proposed BSCR. The remainder of the paper is structured as follows: Section 2 provides background on the balanced scorecard, the board's role, and cyber resilience. Section 3 summarizes the research methods used in this study. Section 4 highlights key findings from the data that informed the BSCR. Section 5 presents the conceptual framework of the BSCR. Section 6 discusses the framework's use and Section 7 has conclusions.

2. Background Literature

As foundation for this research, two areas of literature are summarized. First, this work draws from literature about the balanced scorecard initially developed to support financial reporting. Next, this work draws upon previous studies of BODs role in cybersecurity governance.

2.1 Balanced Scorecard

The initial concept for a balanced scorecard for cyber resiliency (BSCR) is based on the balanced scorecard introduced in the seminal Harvard Business Review article by Kaplan and Norton (Kaplan & Norton, 1992). To address investor decision-making and emerging competitive landscape (Ernst & Young, 1998), the balanced scorecard incorporated important performance indicators about customers, business processes, learning and growth. As described by the founders: “The balanced scorecard is like the dials in an airplane cockpit: it gives managers complex information at a glance” (Kaplan & Norton, 1992). In 1996, Kaplan & Norton extended its theoretical foundation, linking between measures and remodeled balanced scorecard as a strategic management tool to help translate strategy into action (Kaplan & Norton, 1996). This version of the balanced scorecard consists of four main pillars – financial, customer, learning and growth, and internal business process (Kaplan & Norton, 1996).

The primary purpose of the original balanced scorecard was to provide insight into financial and operational performance by combining information about core activities that are otherwise isolated from each other. The aim was to create insights to high-level results through a framework that gathered insights from each component (Kaplan & Norton, 1996). The critical information conveyed by the balanced scorecard provided a view of measurement and management that included operational, financial, and other metrics into a single framework that helped measure the company’s driving future performance. The research described here extends the original concept of the balanced scorecard to cybersecurity governance by considering the components relevant for cyber resiliency and developing a link between measurable cybersecurity drivers and the strategic business goals of the organization (Pearlson et al., 2020).

2.2 Board's Role in Cybersecurity Resilience

Two of the primary responsibilities of the board of an organization are corporate governance and overseeing risk management (Milică & Pearlson, 2023). Until recently, most boards viewed cybersecurity as an infrastructure or operational decision, perhaps even just a technology decision. Boards rarely discussed cybersecurity, and when they did, discussions were highly technical in nature, justifying asks for additional spend, or to review protections and controls in place to meet regulatory requirements (Osterman Research, 2016).

But the continued headline-making data breaches, the increased spending on cybersecurity resources, and new regulatory activity have made cybersecurity and cyber risks top issues for BODs (Milică & Pearlson, 2023). Research shows that there has been a surge in cybersecurity spending by companies worldwide. For example, Gartner (Gartner, 2022) forecasts the global cybersecurity spending will exceed $188.3 billion by the end of 2023, which is 11.3% growth from 2022.

Further, recent regulatory activity has forced BODs to pay attention to cybersecurity. Incident reporting, board expertise, and the board's role in cybersecurity oversight, and ensuring reasonable cybersecurity activities are among the topics of recent rulings by the U.S Security Exchange Commission (SEC) (Securities and Exchange Commission, 2022). These SEC raise concern for BODs of publicly traded companies, and by extension companies doing business with them. BODs are concerned about how their organizations are keeping cybersecure and cyber-resilient. This same regulation and many others

impose hefty fines for non-compliance. (Securities and Exchange Commission, 2022). According to Accenture's State of Cybersecurity Report (Accenture, 2021), 70% of the organizations now include cybersecurity as an item for discussion in every board meeting indicating the change in focus: cybersecurity has become a top concern for business leaders.

But the way cybersecurity is viewed, reported, and discussed in most boards is inadequate for proper oversight and board governance. Osterman Research found that more than half (54%) of board members agreed that the cybersecurity reports are too technical (Osterman Research, 2016). An additional study of US corporate directors found that only 53% thought their board "somewhat understand" cybersecurity (PwC, 2021). By focusing on cybersecurity as a technical, or an infrastructure, investment, boards are not having the right conversations about resilience, business risk, strategic importance, or continuity (Milică & Pearlson, 2023). The result is an imbalance in cybersecurity resource allocation, favoring protection at the expense of recovery and response. Cybersecurity vulnerabilities, and hence business risk, can come from organizational, supply-chain, and financial decisions, not just technology decisions. Since cybersecurity vulnerabilities and threats are constantly changing, organizational focus must also shift from primarily protection to resilience to ensure organizations are minimally impacted by dynamic threats and breaches (Milică & Pearlson, 2023). To make the appropriate decisions for resilience, boards need different information than they receive in the technical reports given to them today.

There have been studies which have identified cyber risk dashboards to address dynamic (Zeijlemaker et al., 2022) and strategic cyber risk challenges (Pearlson et al., 2020). For example, the Exploring Cyber International Relations (ECIR) research project (Madnick et al., 2009) provided a set of analytical tools for understanding and managing cyber security. It provided a dashboard for scholars, policymakers, IT professionals and other stakeholders with a comprehensive set of data on national-level cyber security, information technology and demographic data (Madnick et al., 2009).

While these dashboards provide useful information for understanding investments in protection, they do not provide the necessary information for board evaluation of risks to cyber resilience. They often report on the status of controls, the justification of expenses to increase protections, and the investments to combat known vulnerabilities. They do not report on resilience.

Further, reports to boards do not contain information useful, or even understandable, by non-technical directors. The information is too technical and granular for boards to use to evaluate resilience. For example, by reporting the results of phishing tests and the risk of an employee clicking on a rogue email, the board is left making the connection between this information and organizational resilience. There is a gap between the information provided to boards today and the information boards need to ensure cyber resilience.

To summarize, there are at least two problems with existing cybersecurity tools available to BODs. First the focus is on protection rather than cyber resilience. Most of the information reported to boards is about technology investments and cybersecurity controls, not the business risk to resilience and avenues taken to mitigate that risk. Second the tools are too granular and complicated. Most of the reports focus on technology performance indicators and operational measures more useful for day-to-day management done by CISOs and cybersecurity managers than for oversite done by boards. Since there are no well-established and broadly accepted performance indicators for evaluating cyber resilience, Boards need a tool that provides them information to enable oversite and evaluation of decisions made by operational managers.

3. Research Methods

The review of relevant literature demonstrated that cybersecurity reporting to the BOD is incomplete due to two key reasons – (1) It does not provide the right business context, and (2) It provides indicators of protection and not resilience. As a result, the goal of this theory building project was to create a balanced scorecard for cyber resilience (BSCR) using an exploratory and qualitative methodology for gathering and analyzing data (Billups, 2019).

To provide a deep and meaningful understanding of cybersecurity information at the board level, 16 in-depth semi-structured interviews with CIOs, existing board members in US organizations across diverse industries were conducted. These were supplemented with two detailed surveys and two focus groups of cross-industry executives and subject matter experts.

An initial survey provided a list of cybersecurity key performance indicators and metrics (KPIs), then asked 11 cybersecurity leaders which they reported to their boards and what their boards wanted to know. Analysis of the responses indicated that this approach made too many assumptions about appropriate metrics and asked about inappropriate KPIs for board oversight. The initial results indicated that this was the wrong approach to understand how boards assess cybersecurity risk and resilience.

Based on the inadequate information obtained from the first survey, a second survey was developed

with more open-ended questions about operational, financial, technical, supply-chain, and organizational risk. The new survey used open ended questions such as: (1) What does the board need to know to assess operational / financial / technical / organizational risk due to cybersecurity vulnerabilities? (2) What does board need to know to assess overall organizational resilience to cybersecurity vulnerabilities? (3) What questions does the board ask of the cybersecurity leaders in their board meetings? This survey was administered to a different group of cybersecurity leaders, and 25 responded. This approach yielded a rich qualitative dataset that formed the BSCR development.

Once an initial board-level BSCR was created, focus groups were used to evaluate and socialize the framework. Information collected from the focus groups included comment about the components included in the scorecard, its usefulness to boards, and operational data that might inform or back up the board level BSCR.

4. Qualitative Data and Findings

Since the qualitative findings were highly insightful, they provided guidance for the design of the BSCR. All respondents had strong opinions about cybersecurity boardroom discussions. Generally, participants agreed that BODs had a difficult time discussing cybersecurity at a meaningful level, the board needed different information, and a new approach was necessary. For example, one responded commented,

"*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.*"

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 mentioned who was a board member of a technology services company remarked as follows,

"*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. One of the board members currently serving on a real estate firm mentioned,

"*I'd like to know more about the cost of business interruption, e.g., lost profits; financial liability to third parties, due to cyber breaches.*"

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 risk details should be part of the oversight for the board. For example, one respondent said,

"*Not sure that technology or supply-chain risks are part of the mission of the board as oversight. Max for me would be a yearly interview with an external technical auditor.*"

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 employee's skills to handle potential organizational vulnerabilities. One of the board members from a major firm commented,

"*How is our organization monitoring organizational and people risk? Regulatory feedback. But maybe we need something better.*"

Interviews revealed that boards frequently delegate responsibility of cybersecurity to audit and risk committees. Respondents commented that feedback from these committees would be 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. Respondents mentioned that financial, supply-chain, technological and organizational risk assessment might lead them draw inferences to overall organizational resilience. One of the respondents who identified as a cybersecurity experts commented,

"*At present the Board can only rely on tests carried out by the IT department. This is not sufficient, and external cybersecurity advisers are being considered to provide a more complete picture of cyber resilience.*"

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 commented,

"*My board is interested in resilience, but also curious about what others are doing. They value peer insights and comparisons.*"

Finally, respondents commented that discussions about resilience were needed at the board level, and that there was a lack of tools to help boards perform appropriate cybersecurity oversight.

5. The Balanced Scorecard for Cyber Resilience (BSCR)

Previous research and insights from the primary data collected for this study highlighted the need for a comprehensive, balanced approach to managing and reporting cyber risk in a manner consistent with what boards need. That is the goal of the Balanced Scorecard for Cyber Resilience (BSCR). The BSCR presents an aggregated view of cyber resilience based on key aspects of cybersecurity risk, a qualitative assessment of the most significant risks faced by the organization, and a high-level summary of the action plan to manage those risks. Supporting the BSCR are several levels of detail based on CISA's Cybersecurity Performance Goals (Cybersecurity Performance Goals, 2021).

The conceptual model of the board level BSCR is shown in Figure 1. It combines financial, technological, organizational, and supply-chain assessments with an aggregated indicator of cyber-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 (a 'stoplight' or Green, Yellow, Red scale) for quick assessment of the status of quantitative metrics in that area. These four quadrants were chosen are based on findings from current research that indicated they were the key business risk areas today. But the design makes it possible to customize the BSCR with new or additional key risk areas in the future.

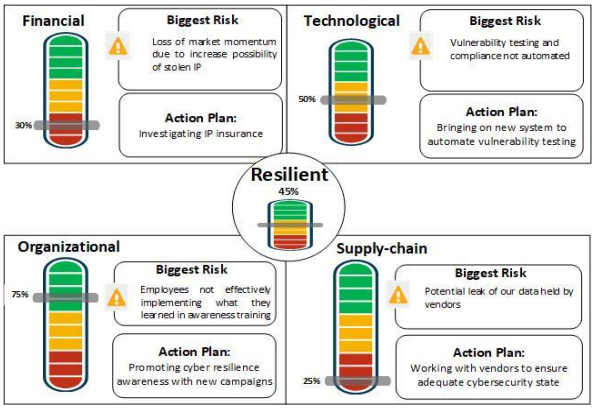

Figure 1. Conceptual model of board level balanced scorecard for cyber resilience for an organization.

Each quadrant of the board level BSCR is designed to provide directors with clear, understandable, relevant indicators of the strength of resilience from that area. The stoplight indicator is quickly understood indicator of how well quantitative cyber risk indicators meet expectations (discussed in Section 5.1). The *Biggest Risk* box is a qualitative assessment made by knowledgeable cybersecurity leaders, such as the CISO or CIO, of the most problematic issue in that area. The *Action Plan* box is the leader's high-level plan to manage the biggest risk. The *Resilient* indicator in the center of the balanced scorecard is an overall assessment of the organization's cyber resilience based on the four quadrants. This structure provides directors with relevant and quickly understandable information based on both qualitative inputs from managerial insights and quantitative inputs from cumulative data. The goal is to both inform the BOD and to spark deeper conversations with operational managers.

5.1 The Four Quadrants

The information presented in the board level BSCR is derived from qualitative and quantitative assessments of cybersecurity resilience and risk. Figure 2 illustrates a comprehensive, but representative, sample of information that feeds into the board-level BSCR. Figures 3, 4, 5 and 6 magnify each of the areas for additional clarity.

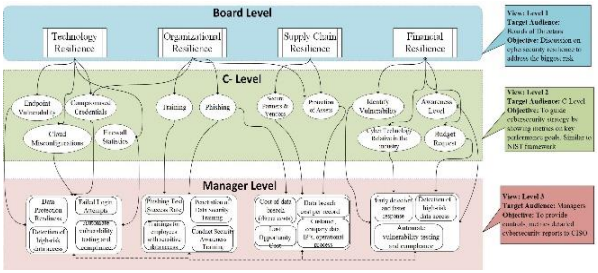

Figure 2. Levels of information supporting the BSCR

The stoplight indicator in each quadrant is a function of the key performance indicators, targets, and objectives set by management. The information used to calculate the stoplight indicator comes from operational data collected from systems, assessments, and investments. Operational managers may have their own cyber security data collected from their security operations, but one source used for illustrative purposes is the CISA CPG (Cybersecurity Performance Goals, 2021). Thresholds would be established for each color based on a score calculated from measures at more operational levels. If the top

of the scale is 100%, indicating the highest-level operational managers believe is possible for resilience, then the sliding indicator would show the board how close KPIs are to this level. For example, the colors might represent:

- Green = High, Actual vs Target is above 65%
- Yellow = Actual vs Target is between 35% and 65%
- Red = Low, Actual vs Target is below 35%

5.1.1 Technology Quadrant. Most organizations have invested in technologies to keep their organizations secure, such as firewalls, identity and access management tools, security operations monitoring, and penetration testing tools. For many boards, the reports they receive are primarily about the performance and effectiveness of these tools. Understanding these investments is a component of the risks that the organization faces from a technology perspective, but the report to the board in the BSCR is the most urgent or largest risk and the plan to address it. This quadrant of the BSCR indicates how well operational leaders are managing technology risk. This quadrant's stoplight indicator can include cybersecurity technology audits, penetration testing results, and many other relevant technology-based metrics. For example, some CISA-CPG practices (Cybersecurity Performance Goals, 2021) to include in the indicator are: (a) incident has response plans that they maintain, practice, and update for relevant threat scenarios. (b) system backups are in place to minimize data loss and security delivery disruption. (c) network controls, segmentation, and topology are documented, implemented, and properly managed. (d) threat detection systems are implemented to detect relevant threats. (e) email security tools are implemented to reduce compromised emails, phishing, and interception of emails and (f) vulnerability scanning, disclosure, and reporting tools and processes are in place. Figure 3 shows how these details might flow up through operational levels to the board level BSCR.

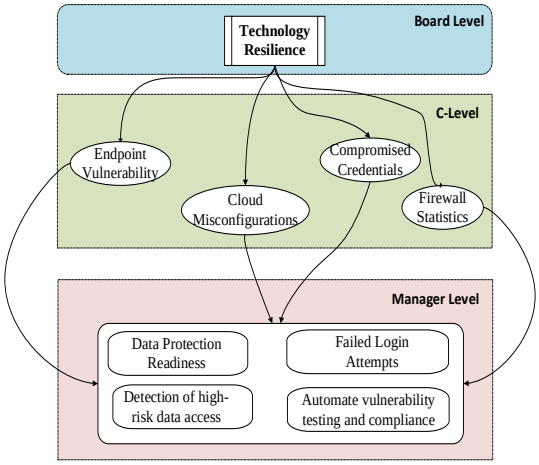

Figure 3. Example of technology resilience information flow from Figure 2 (magnified)

5.1.2 Financial Quadrant. Managing cybersecurity risk means the organization's financial processes are resilient, cash flow is preserved, and expenses are appropriately managed. The board creates financial objectives and uses financial measures in their oversight role. The financial quadrant helps understanding what cybersecurity risks mean to the financial aspect of an organization and how those risks are managed is a critical board-level conversation. Boards have numerous financial health indicators, many of which are appropriate starting points to populate the stoplight indicator for this quadrant. Some of the KPIs that might be part of this quadrant are: (a) investment spent on cybersecurity (budget compared to actual), (b) unanticipated expenses needed to manage a cyber breach, the value of financial assets at risk if there was a cyber breach, (c) comparison of cybersecurity spend (to previous periods and/or to industry) and (d) insurance costs for

cyber coverage. Figure 4 shows how these KPIs contribute to the board level BSCR.

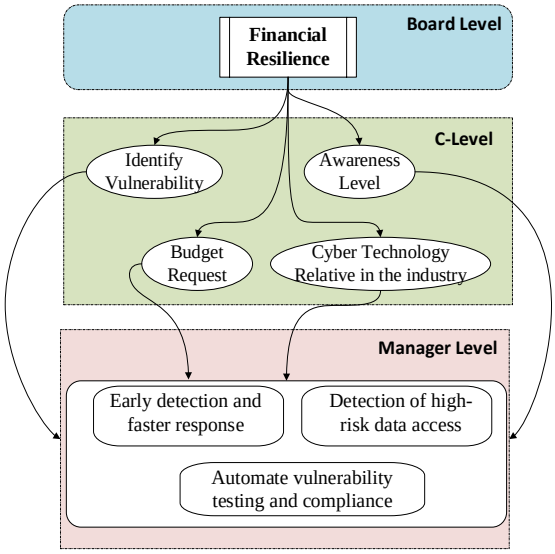

Figure 4. Example of financial resilience information flow from Figure 2 (magnified)

5.1.3 Organization Quadrant. The cyber risk from the organization, specifically the employees, contractors, managers, leaders, and even the board of directors, continues to be one of the biggest vulnerabilities cyber leaders face (Verizon, 2023). This quadrant of the BSCR indicates how well operational leaders are managing this risk. Directors must understand the biggest risk operational leaders expect and evaluate what leaders are doing about it. More quantitative KPIs would be used for the stoplight indicator. For example, the CISA-CPG practices (Cybersecurity Performance Goals, 2021) relevant to this quadrant are: (a) single leader is responsible and accountable for cybersecurity within an organization. (b) single leader is responsible and accountable for OT-specific cybersecurity within an organization with OT assets. (c) organizational users learn and perform more secure behavior. (d) personnel responsible for securing OT assets received specialized OT-focused cybersecurity training and (e) improving IT and OT cybersecurity relationships. Figure 5 shows how this level of detail is represented in the BSCR.

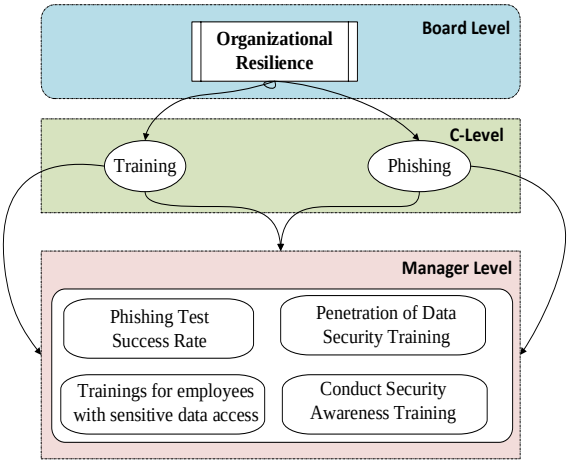

Figure 5. Example of organizational resilience information flow from Figure 2 (magnified)

5.1.4 Supply-Chain Quadrant. A more recently identified source of cyber risk is the organization's supply chain. Vendors increasingly introduce vulnerabilities, and understanding how this risk is mitigated is an appropriate board-level discussion. As with the other quadrants, operational leaders understand the sources of the risk and have an action plan to mitigate that risk. Operational supply-chain resilience might be represented by the stoplight indicator with assessments of components from CISA-CPG (Cybersecurity Performance Goals, 2021) to include: (a) the status of the supplier's cybersecurity plans. (b) supply-chain incident reporting of incidents well-articulated and (c) supply-chain vulnerability disclosure processes in place. Figure 6 shows how this detail informs the higher levels of the BSCR.

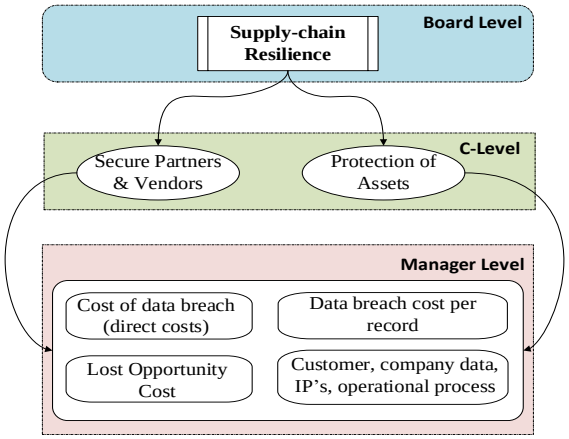

Figure 6. Example of supply-chain resilience information flow from Figure 2 (magnified)

5.2 Overall Resilience

As an overall indicator of cybersecurity resilience, the BSCR includes one stoplight indicator based on the resilience of the four other quadrants. Many researchers have studied the optimal measure of cyber resilience (Zeijlemaker et al., 2022), and those formula might be used here. But this paper proposes an easily understood stoplight indicator based on a simple averaging of the scores from the other quadrants. This indicator would provide an initial assessment to encourage further exploration by the board:

Overall Resilience = f (financial, technological, organizational, supply-chain resilience)

6. Discussion

Boards need a new way of reporting cyber security assessments. Current approaches are at the wrong level, reporting technical KPIs from metrics of protection measures, not on resilience or business risk. Boards are experts at understanding and interpreting quantitative information. When presented with this type of detail, boards focus on the wrong level of detail, at the expense of more relevant discussions, such as risk mitigation, business recovery, and cyber resilience. While quantitative metrics and technical indicators are attractive, perhaps even seductive to directors who favor quantitative data, making the connection from this type of data to conclusions about organizational resilience may be difficult if even possible. It misses the business context, the operational managers expertise about organizational capabilities, and the potential for responding and recovering from a cyber incident. In short, current approaches miss giving BODs information about the biggest risks anticipated from a cyber incident and what mitigations are in place to respond. Boards need this rich information to decide if operational managers have made the best decisions.

While the qualitative assessment of the biggest risks and action plans is the new idea in this theory building work, presenting it in a balanced scorecard gives Boards the information they need to decide if the most cyber-vulnerable areas of the business are managed appropriately. Looking at business risk to technology, financial, organizational and supply-chain aspects of the business allow directors to evaluate a how resilient the organization is to a cyber incident.

Directors must be knowledgeable participants in cybersecurity discussions. Yet often C-level cyber leaders struggle to find the right level of information to report. Being a knowledgeable participant in cyber discussions does not mean directors have to be cybersecurity professionals or experts. But it does mean they must be presented with the right information to make the right type of decision. Understanding of how well protected an organization is will not ensure that the organization is cyber-resilient. Directors need the information about the biggest vulnerabilities or risks their organization faces given all the investments in protection already made. Often that is a qualitative assessment from operational leaders. That knowledge must seed the board-level discussions.

Boards need operational executives to articulate the biggest risk they see in each area and the plan for mitigating that risk. Once the risks are visible, informed directors, subcommittees, or even external experts can dive deeper into the technical details to learn more and to provide oversight into the risks reported. The BSCR seeds the discussion with operational managers by highlighting major business risk in financial, organizational, technical, and supply-chain areas of the business.

The goal of the board level BSCR is to spark relevant, meaningful discussions with operational cybersecurity leaders. This begins with the initial setup of the BSCR. Operational leaders and management must set up the targets and actual metrics to combine into the stoplight indicators. That activity is another way the BSCR seeds discussion with knowledgeable board members and outside experts. Setting up the thresholds for stoplight levels and establishing a reasonable measure for 100% in each category is also a topic for future research.

7. Conclusion

When CISOs and CIOs present technical details, such as percentage of employees failing a phishing exercise or vulnerable endpoints in the system due to a penetration test, the board discusses them. But that does not mean boards are having the right discussions. This paper argues that to meet the board's responsibility to perform oversight and fiduciary responsibility, directors need a different kind of information than the operational details CISOs and CIOs require to manage day-to-day decisions about cybersecurity. The information needed by directors must be in a suitable format, at the right level, and on the relevant subjects. Directors need qualitative assessments of the biggest risk their organizations face given current cybersecurity investments, and the operational leaders plans to mitigate that risk. They also need a quick, high-level indicator of the status of controls, compliance and other quantitative metrics compared to targets.

Boards must make sure their organization has a safe, protected, resilient foundation, and that risks to the business are appropriately mitigated. Boards

provide oversight to ensure their organizations can continue to operate and be successful even in the event of a cyber incident. To do so, they need a balanced view of how cyber incidents may threaten business continuity and a balanced view of how the organization is cyber resilient. The BSCR provides that view.

References

Accenture. (2021). *How aligning security and the business creates cyber resilience.* https://www.accenture.com/_acnmedia/PDF-165/Accenture-State-Of-Cybersecurity-2021.pdf

Billups, F. (2019). *Qualitative data collection tools: Design, development, and applications.* Sage Publications.

Coden, M., Reeves, M., Pearlson, K., Madnick, S., & Berriman, C. (2023). *An Action Plan for Cyber Resilience.* MIT Sloan Management Review. https://sloanreview.mit.edu/article/an-action-plan-for-cyber-resilience/

Cybersecurity Infastructure & Security Agency. (2021). *Cross-Sector Cybersecurity Performance Goals.* Cross-Sector Cybersecurity Performance Goals: https://www.cisa.gov/cross-sector-cybersecurity-performance-goals

Cybersecurity Performance Goals. (2021). *CISA CPG Checklist.* https://www.cisa.gov/sites/default/files/2023-03/cisa_cpg_checklist_v1.0.1_final.pdf

Deloitte. (2021). *The changing role of the board on cybersecurity*. https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-ra-changing-role-of-the-board-on-cybersecurity-noexp.pdf

Ernst & Young. (1998). Measures that matter. *Cambridge, MA: E&Y Center for Business Innovation*, *26*(2). https://doi.org/10.1108/eb054615

Gartner. (2022). Worldwide Security and Risk Management Spending to Exceed $150 Billion in 2021. https://www.gartner.com/en/newsroom/press-releases/2021-05-17-gartner-forecasts-worldwide-security-and-risk-managem

Kaplan, R., & Norton, D. (1992). The balanced scorecard — Measures that drive performance. *Harvard Business Review*, *70*(1), 71-79. https://www.scopus.com/home.uri

Kaplan, R., & Norton, D. (1996). Using the balanced scorecard as a strategic management system. *Harvard Business Review, 74*(1), 75-85. https://www.scopus.com/home.uri

Madnick, S., Choucri, N., Camina, S., Fogg, E., Li, X., & Fan, W. (2009, September 23). Explorations in Cyber International Relations (ECIR) - Data Dashboard Report #1: CERT Data Sources and Prototype Dashboard System. *MIT Sloan Research Paper, 4754*(09). http://dx.doi.org/10.2139/ssrn.1477618

Milică, L., & Pearlson, K. (2023, May 02). Boards Are Having the Wrong Conversations About Cybersecurity. https://hbr.org/2023/05/boards-are-having-the-wrong-conversations-about-cybersecurity

Osterman Research. (2016). *How Boards of Directors Really Feel about Cybers Security Reports.* https://sicccIber.com.br/wp-content/uploads/2019/03/how-board-of-directors-feel-about-cyber-security-reports-1.pdf

Pearlson, K., Saunders, C., & Galletta, D. (2020). *Managing and Using Information Systems: A Strategic Approach* (7 ed.). John Wiley & Sons.

PwC. (2021). *PwC's 2021 Annual Corporate Directors Survey (The director's new playbook: taking on change.* https://www.pwc.com/us/en/services/governance-insights-center/assets/pwc-2021-annual-corporate-directors-survey.pdf

Securities and Exchange Commission. (2022). Cybersecurity Risk Management, Strategy, Governance and Incident Disclosure. *Federal Register, 87*(56). https://www.govinfo.gov/content/pkg/FR-2022-03-23/pdf/2022-05480.pdf

Tosun, O. (2021). Cyber-attacks and stock market activity. *Science Direct, 76*(2021). https://doi.org/10.1016/j.irfa.2021.101795.

Verizon. (2023). DBIR- Data Breach Investigation Report.https://www.verizon.com/business/resources/T48e/reports/2023-data-breach-investigations-report-dbir.pdf

Zeijlemaker, S., Siegel, M., & Dobrygowski, D. (2022, Nov 15). *World Economic Forum*. As cyber attacks increase, here's how CEOs can improve cyber resilience https://www.weforum.org/agenda/2022/11/as-cyber-attacks-increase-heres-how-ceos-can-improve-cyber-resilience/