Cyber Warrior or Cyber Washing? Examining the Expertise of Board Members Serving on Cybersecurity Committees

Abstract

In the face of the growing cybersecurity risks facing today's organizations, many boards of directors are forming cybersecurity committees to help navigate the associated governance issues. However, the optimal skill set for a prospective cybersecurity committee member remains unclear. In response, we draw on expertise theory to investigate if the background of board members serving on cybersecurity committees is sufficient to fulfill their governance responsibilities. We examine the education, work experience, and training of 239 cybersecurity committee members across 62 firms and find that most directors are experienced board members and/or business executives, but very few have expertise in cybersecurity. Our results highlight concerns in the ability for cybersecurity committees to adequately oversee cybersecurity risks at their organizations and we offer a series of recommended actions for boards to undertake in response.

Introduction

Boards of directors are increasingly concerned with the continued risks posed by cybersecurity threats (Milică & Pearlson, 2023) and are subject to expanding regulatory requirements mandating board involvement in cybersecurity governance (Deloitte, 2021; Proudfoot et al., 2023). As a result, many boards are turning to specialized cybersecurity committees to help navigate the related governance challenges (Deiso, 2022; O'Donnell-Welch, 2023). However, boards are still struggling to determine the optimal skill set for prospective committee members and are experiencing challenges in recruiting candidates (Nash, 2023; NightDragon, 2023; Violino, 2023).

For example, a recent report finds that 67% of executives perceive their board's expertise on cybersecurity issues to be either fair or poor (PwC, 2023), even though it is "important that the board has the skills and expertise needed, or has access to skills and expertise, to oversee this area" (PwC, 2024, pp., p. 15). Board-level cybersecurity expertise allows directors to lead meaningful discussions about the firm's risk-related decisions, governance, and accountability (Chickowski, 2023). Specifically, "a board director with deep cybersecurity expertise can collaborate closely with senior management and IT teams and provide valuable insights into identifying vulnerabilities, assessing risk, and developing solutions. They can also play a critical leadership role in overseeing regular security audits, ensuring that contracts associated with business objectives are reviewed for cybersecurity implications, and helping the IT team navigate incident response efforts alongside other teams, such as legal" (Abraham et al., 2024, p. 2). Similar arguments in favor of domain-specific expertise for board members were made following the passage of the Sarbanes-Oxley Act in the context of finance and accounting knowledge (Defond et al., 2005).

We approach this pressing corporate governance challenge from the perspective of expertise theory, by suggesting that in order to adequately oversee cybersecurity activities, cybersecurity committee members should have at least some domain-specific education, experience, and/or training. In doing so, we pose the research question: Do current cybersecurity committee members have sufficient domain expertise to fulfill their governance responsibilities?

To evaluate the current state of cybersecurity committee members' expertise, we collected data from 239 cybersecurity committee members across 62 firms, focusing on their experience, education, and training. Our results reveal that most cybersecurity committees are comprised of experienced board members and executives, but very few can be categorized as cybersecurity experts.

Our findings bring into question the value that cybersecurity committees—with their current membership—actually contribute to advancing board governance. Although the creation of cybersecurity committees sends a positive signal to stakeholders that the board recognizes the criticality of cybersecurity risks

(alluding to the "cyber warrior" label in our study's title), we believe that those same stakeholders would be surprised to learn how few committee members were truly experts in the area. This observation gives rise to our "cyber washing" label, which adapts the widely used green washing label used for companies emphasizing observable aspects of corporate social responsibility, while neglecting unobservable aspects (Wu et al., 2020).

Our results yield three key contributions. First, we draw on the expertise and corporate governance literature to frame an approach for evaluating the suitability of board members to serve on the cybersecurity committee based on domain-specific education, experience, and training. Second, we reveal the disconnect between firms that establish cybersecurity committees, but then fail to nominate board members with an appropriate level of domain-specific expertise. This reiterates ongoing concerns regarding the capability of boards to adequately oversee cybersecurity activities. Third, our research serves as a call to boards to not only "talk the talk" on addressing cybersecurity risks but also "walk the walk" by endeavoring to nominate at least one domain expert to their cybersecurity committee. We provide a series of recommendations to help advance this goal.

Background

The board of directors serves the corporation and its shareholders in overseeing and monitoring management, providing advice (e.g., on risk), and helping to set the organization's strategic direction. (Adams et al., 2010; Héroux & Fortin, 2024). Board members can be categorized as either *inside* directors, who are firm employees such as the CEO, or *outside* directors, who are independent of the firm.

Board committees are set up to address particular areas of risk and assist the board by focusing on particular organizational activities (Adams et al., 2010). For U.S. public companies, committees for audit, compensation, and nominating/governance are required, but additional standing committees (i.e., formally defined, continually used) such as strategy and finance are routinely set up (Chen & Wu, 2016). Although the typical board composition may represent a broad set of director experiences in general management, finance, and strategic issues, one area of particular concern in recent years is the lack of expertise related to technology in general, but cybersecurity specifically (Larcker et al., 2017).

The Emergence of the Cybersecurity Committee

Although technology issues have played an increasingly important role in board discussions of late, much of the oversight responsibility is often subsumed by a broader committee, such as the audit committee. However, over the past decade, stand-alone technology committees have been established to provide more focused oversight of the firm's IT governance (Czarnecki, 2015), which refers to "the exercise of decision rights, and the design and execution of structures and processes to ensure strategic decision making designed for delivering IT value, accountability, and integrity" (Price & Lankton, 2018, p. 109). Recent estimates suggest that approximately 12% of global Fortune 500 firms have a board-level technology committee (Forrest et al., 2022). Past research finds that forming a technology committee positively relates to both corporate governance and performance metrics (Premuroso & Bhattacharya, 2007).

However, as specific risks around cybersecurity have grown, audit and technology committees have begun to struggle with the added complexity (Center for Audit Quality, 2023; Hitchcock et al., 2017; Lanz, 2014; Lowry et al., 2021). In response, many firms are creating a new, stand-alone cybersecurity committee. Doing so sends a signal to stakeholders that the board appreciates and is prepared to oversee cybersecurity issues, as well as enhance the level of cybersecurity disclosures in financial regulatory findings (DeMayo & DeLena, 2024; Héroux & Fortin, 2024). However, reports suggest that boards are struggling to determine the optimal skill set for prospective committee members and are experiencing challenges in recruiting candidates (Bandodkar & Grover, 2022; NightDragon, 2023; Violino, 2023).

Committee Members' Literacy & Expertise

Past research on the importance of domain-specific committee members' literacy and expertise is common within the corporate governance literature generally (e.g., Adams et al., 2010), as well as in the accounting literature regarding the audit committee (e.g., Bédard & Gendron, 2010; Couchoux, 2024).

In general, directors with subject matter expertise are highly valued. For example, Boivie et al. (2021) suggest that "having directors with expertise and motivation to ask strategically relevant questions during board meetings can be an important mechanism to board effectiveness" (p. 1686). Similarly, Baysinger and

Butler (2019) suggest that "shareholder welfare is enhanced by boards of directors which are capable of monitoring management, rendering independent judgments on managerial performance, and meting out rewards on the basis of these evaluations" (p. 103).

Similarly, McDaniel et al. (2002) find that financial experts on the audit committee are more likely to raise concerns around reporting quality, as well as recurring activities, relative to those members that are only financially literate. For instance, in the United States, audit committee members of publicly listed companies are required to be financially literate and at least one member of the committee is required to be a financial expert (Couchoux, 2024; McDaniel et al., 2002). In this context, financial experts are desired by audit committee chairs, albeit with a diversity in backgrounds and skills (Free et al., 2021).

From a technology committee standpoint, commentators have recommended that at least one member be an IT expert, such as a CIO or an active IT manager (Caluwe & De Haes, 2019; Czarnecki, 2015; Nolan & McFarlan, 2005), even though committee charters do not often specify such requirements (Price & Lankton, 2018). However, Digital Directors Network CEO and retired PwC partner Bob Zukis notes that "bringing in technology/cybersecurity experts to the boardroom has been glacial. It's starting to move, but boards can't govern what they don't understand" (Ferracone, 2019, p. 3).

Recent regulatory changes by the U. S. Securities and Exchange Commission (2023) have further drawn attention to cybersecurity expertise on the board. Specifically, Item 106 and Item 16k in the Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure guidelines require a description of the board's oversight of cybersecurity risks, the identification of the committee responsible for cybersecurity risk oversight, and a description of management's role in assessing/managing cybersecurity risks. Although there had been a provisional requirement that would have required public companies to disclose information on the type of cybersecurity expertise held by board directors, this condition was removed in the final version of the regulation (NightDragon, 2023)

Despite the growing importance of cybersecurity risks, subject matter literacy or expertise is not a core qualification for most board members (Larcker et al., 2017). This reality is reflected in recent reports of many directors lacking basic cybersecurity understanding (PwC, 2023). Similarly, Lowry et al. (2021) find that less than 15% of a sample of Russell 3000 firms disclose that none of their directors has cybersecurity expertise. Although firms struggle to place cybersecurity experts on boards, past research confirms that "the level of individual directors' cybersecurity expertise is an important determinant of the effectiveness of board oversight…when boards lack directors with cybersecurity expertise, they are less likely to substantively address cybersecurity during board meetings" and that "cybersecurity expertise affects the quantity, quality, and depth of the questions that directors ask cybersecurity executives as well as their ability to meaningfully respond to answers received" (p. 3).

Research model

We approach the question of whether current cybersecurity committee members have sufficient expertise to fulfill their governance responsibilities by drawing on past work on expertise theory. In particular, we focus on what characterizes expertise in a cybersecurity context and how such expertise can aid in governance activities.

Seminal research on expertise suggests that the outstanding performance of an individual (relative to others) can be attributed to abilities that are either inherited (e.g., intelligence) or acquired (e.g., knowledge) (Ericsson & Smith, 1991). Of those abilities that are acquired, they can be further categorized as either general learning/experience or domain-specific training and practice (Ericsson & Smith, 1991). Indeed, past research suggests that experts differ from novices in their ability to rapidly access relevant knowledge pertaining to a situation (Chase & Simon, 1973). Further, research finds that training distinguishes experts from novices in making judgments within a wide range of disciplines (Ericsson & Charness, 1994; Garb, 1989). From this perspective, expertise "is a rare skill that develops only after much instruction, practice, and experience. The cognition of experts is much more sophisticated than that of novices; this sophistication is presumed to produce better predictions" (Camerer & Johnson, 1991, p. 195).

In the context of corporate governance, board-level expertise is often alluded to in terms of an individual's education, experience, and training (Jewer & McKay, 2012; Vincent et al., 2019). This perspective is in line with views on cybersecurity expertise, where Lowry et al. (2021) suggest that a necessary element of

cybersecurity expertise for a director is actual work in or the overseeing of a cybersecurity function. Similarly, a recent IANS (2023) report highlights desirable traits of cyber-oriented board director candidates, which includes first-hand work in the cybersecurity field and an advanced education.

As such, when appointments are made to the cybersecurity committee, we expect that selections will be made with a strong consideration given to those with domain-specific expertise, which we categorize as at least one of the following: higher education, functional experience, or certifications/training. For education, this includes the attainment of higher education degrees, with specializations in cybersecurity, such as a Master of Science in Cybersecurity Management or a Master of Business Administration in Cybersecurity. For functional experience, this includes roles pertaining directly to cybersecurity, such as a Chief Information Security Officer, Vice President of Cybersecurity, or Cybersecurity Consultant. For certifications/training, this includes the attainment of broad cybersecurity credentials such as the Certified Information Systems Security Professional, Certified Information Security Manager, or CERT Certificate in Cyber-Risk Oversight. On this basis, we suggest the following three hypotheses:

> H1: Boards of directors will appoint cybersecurity committee members with cybersecurity-specific higher education credentials.
>
> H2: Boards of directors will appoint cybersecurity committee members with functional cybersecurity experience.
>
> H3: Boards of directors will appoint cybersecurity committee members who have completed practical cybersecurity certifications and/or training programs.

Methodology

To examine our research question, we first obtained a list of firms that have formed a board-level cybersecurity committee. We drew on two sources to compile this list: the Board and Directors Committee dataset from BoardEx and the Director and Officer Changes data from Audit Analytics. We filtered for firms that included the keywords "Cyber" or "Cybersecurity" in the committee's name. Our search was conducted for data until the end of 2023. We reviewed the results from each search and removed duplicates.

For each identified cybersecurity committee, the BoardEx and Audit Analytics databases provided basic director-level data (e.g., director names, if the director was independent, if they chaired the committee). In order to supplement this data, we manually searched each firm's annual proxy statement to confirm the creation of the cybersecurity committee and the identity of the directors serving on the committee. Further, we used the annual proxy statements to collect information on committee-level characteristics (e.g., number of members serving on the committee) and director-level characteristics (e.g., education, experience, certifications, gender, age). Please refer to Table 1 for a listing of the data collected. If the annual proxy statements did not provide the necessary information, we used LinkedIn and other corporate websites as supplemental sources. In cases where we could not obtain the necessary information (i.e., missing education details, missing proxy statements, unclear committee membership), we removed the entry from our analysis. For situations where a director served on a cybersecurity committee at more than one firm (this was the case for 10 directors), we counted the director only once for individual-level analysis, while also including the director's data for all committee-level analysis. Our final sample consists of 239 directors spanning 62 firms.

Table 1: Collected Data

Variable	Description	Source
Committee name	The name of the cybersecurity committee	BoardEx/ Audit Analytics
Director name	Name of the director serving on the cybersecurity committee	
Committee role	The director's role on the committee (either chair or member)	
Number of members on the committee	The number of board members serving on the cybersecurity committee	
Cybersecurity education	If the board member has completed a cybersecurity-specific higher education degree	Proxy state-ments, external websites
Cybersecurity work experience	If the board member has cybersecurity work experience	
Cybersecurity certification or training	If the board member has completed a cybersecurity-specific certification or training course	

Technology education	If the board member has completed a technology-specific higher education degree	
Technology work experience	If the board member has technology work experience	
Director has executive experience	If the board member has executive level work experience	
Director has board-level experience	If the member has prior experience serving on other boards	
Gender	Gender of the board member	
Age	Age of the board member	

Of particular relevance to our hypotheses is the collection of data relevant to each director's cybersecurity education, work experience, and certification/training. We drew on the principles of expertise theory in selecting these criteria. To fulfill the cybersecurity education criterion, directors needed to have earned a higher education degree (undergraduate or graduate) in a cybersecurity-specific topic, such as a Master of Science in Cybersecurity. To fulfill the cybersecurity work experience criterion, directors needed to have first-hand work experience in a cybersecurity role, such as a CISO, CSO, or cybersecurity consultant. To fulfill the cybersecurity training/certification criterion, directors needed to have earned a recognized industry certification such as a CISSP or CISM, or completed a training course, such as the National Association of Corporate Directors (NACD) CERT Certificate in Cyber-Risk Oversight or the MIT Cybersecurity Leadership for Non-Technical Executives course.

In order to consider the nuances of committee members' expertise, we also collected data on the extent that directors had technology education (e.g., MBA in IT Management) and technology work experience (e.g., CIO, VP of IT, CTO). Although these measures are not directly cybersecurity-specific, there could be some cybersecurity elements that could contribute to an improved appreciation for cybersecurity issues.

Results

From our collected data, we identified 239 directors serving on 62 cybersecurity committees. Of these directors, 161 (67.4%) were male and 78 (32.6%) were female. The directors' ages ranged from 31 to 82, with the average being 59.9 years old. We also found that most cybersecurity committee members had previous experience serving on the boards of other organizations (90.4%) and working in non-technology executive roles such as a CEO, CFO, or COO (84.5%).

However, when we examined the domain-specific expertise of cybersecurity committee members, we were surprised to find that only one (0.4%) director had cybersecurity education, 16 (6.7%) had related work experience, and five (2.1%) had completed cybersecurity certifications/training. On this basis, none of our three hypotheses were supported, where we predicted that boards would appoint members with higher education credentials (H1), functional cyber experience (H2), and cyber certifications or training (H3).

Despite this general lack of cybersecurity-specific expertise, we also examined the level of general (i.e., non-cybersecurity) technology education and work experience of cybersecurity committee members. Here, we found that 40 (16.7%) directors had completed some form of technology education (e.g., MBA in Technology Management) and 51 (21.3%) had direct technology work experience (e.g., CIO, CTO). Please refer to Figure 1 for a comparison of these directors' characteristics.

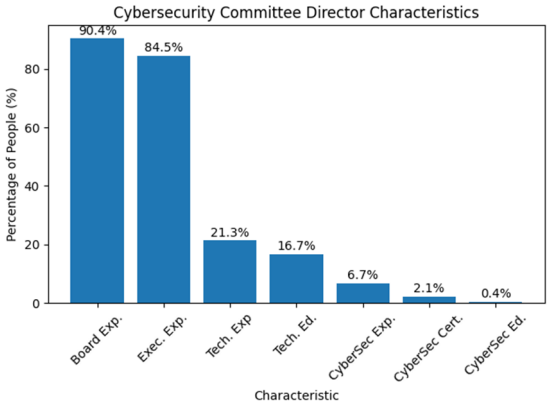

Figure 1: Cybersecurity Committee Directors' Characteristics

Next, we examined our data from the perspective of the 62 cybersecurity committees. We found that the average number of members was 3.5, with the smallest having only a single member and the largest having six members. Forty (64.5%) of the identified committees focused exclusively on cybersecurity (and closely related issues, such as privacy), while the remaining 22 (35.5%) committees focused on both cybersecurity and another broad issue.[1]

At a firm level, only 15 of 62 cybersecurity committees (24.2%) had at least one director with cybersecurity expertise. Of these, four committees (6.0%) had more than one cybersecurity expert. Generally, the chair of the cybersecurity committee had slightly more expertise than non-chair committee members.[2] Specifically, 2.9% of chairs had cybersecurity education (versus 0% of committee members), 11.6% of chairs had domain-specific work experience (versus 4.4% of committee members), and 4.3% of chairs had completed cybersecurity certifications/training (versus 1.1% of committee members).

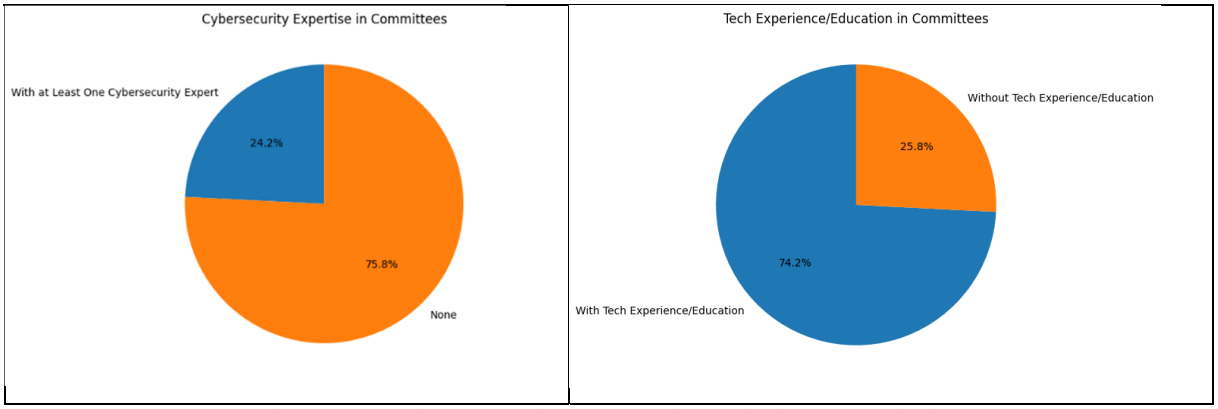

Figure 2: Cybersecurity Committees' Characteristics

We investigated if there were differences in the quantity of experts serving on committees that focused exclusively on cybersecurity issues (relative to those that were responsible for both cybersecurity and another related area). The results suggested that such committees were slightly more likely to have at least one cybersecurity expert (30.0%, compared to 24.2% for all committees). We also examined how many of the 62 cybersecurity committees had at least one director with (non-cybersecurity specific) technology education or work experience. Our results indicated that this was the case for 46 (74.2%) committees. Please refer to Figure 2 for a comparison of these committees' characteristics.

In summary, our results suggest that boards tend to appoint cybersecurity committee members who are experienced business executives and directors. Although relatively few committee members have a general technology background, these directors tend to be spread out, leaving almost three quarters of cybersecurity committees with at least one technology-capable member. However, it is striking how few cybersecurity committee members we consider to be domain experts; we find that more than three quarters of cybersecurity committees have no directors with direct cyber education, work experience, or certifications.

Discussion

Although we find that most cybersecurity committee members have previous experience as board members and business executives, our analysis reveals that less than one quarter of committees have at least one cybersecurity expert. It remains unclear from our results if boards are satisfied with their current cybersecurity committee membership or if they sought out cybersecurity experts and were unsuccessful in appointing them to the board. In at least some cases, it is possible that boards wish to signal to the market that they recognize the importance of cybersecurity risk to the firm by forming a standing cybersecurity committee, but put in little effort to bolster the firm's stance on cybersecurity, such as by simply appointing

[1] Of these 22 committees, 16 were joint "cybersecurity and technology committees," while the remaining committees paired cybersecurity with areas such as risk, innovation, and regulatory compliance.
[2] Our data consisted of 69 chairs and 180 members. This exceeds our total of 239 members as 10 directors served on multiple cybersecurity committees.

existing directors to serve on the committee.[3] Past research on signaling theory suggests that by reinforcing perceptions of a forward-thinking board (e.g., by creating a cybersecurity committee), directors can indicate to stakeholders that they are effectively protecting their interests (Connelly et al., 2011; Héroux & Fortin, 2024; Higgs et al., 2016). However, since the stakeholder recipients of the board's signal may not have access to the information necessary to evaluate the expertise of members of the cybersecurity committee, the actual contribution of the committee may be minimal.

A key question that emerges is whether boards need cybersecurity experts serving on cybersecurity committees to fulfill their governance responsibilities or if experienced, generalist business leaders are enough. The argument in favor of expert directors is that the cybersecurity committee cannot provide effective governance if they have insufficient knowledge of the topic. This view is highlighted by Lowry et al. (2021), who note that a "lack of cybersecurity expertise leads boards to rely heavily on the chief information security officer (CISO) to coach them on cybersecurity concepts, risks, program objectives, and even the process of cybersecurity oversight itself. This reliance on management inhibits the board's ability to provide an independent assessment of cybersecurity risk or to provide incremental value in their oversight" (p. 3). Lowry et al. (2021) refer to this as "circular governance," in that directors become over reliant on the guidance of the managers they are supposed to be overseeing.

Perhaps part of the challenge in determining the adequacy of expertise required is a lack of clarity in terms of what exactly a cybersecurity committee member is responsible for overseeing. As an example, we looked at the proxy statement of one of the firms in our sample, Bill Holdings Inc. (2023). Six cybersecurity committee activities were outlined on pages 19-20:

> 1. Understanding our key risks and the measures implemented by the Company to mitigate and prevent cyber attacks and respond to data breaches;
>
> 2. Assessing our cybersecurity architecture, technology, controls, and policies, as well as overall security culture and employee adherence to best practices;
>
> 3. Overseeing our cybersecurity strategy and technology planning processes in light of the threat landscape facing us and our products, services and operations, including regularly reviewing the results of cybersecurity threat exercises;
>
> 4. Receiving quarterly updates from members of our Executive Security Risk Management Committee, which is comprised of senior members (VP-level or above) of our engineering, legal and compliance, people, operations, risk management, marketing, finance and product departments;
>
> 5. Overseeing our compliance with applicable information security and data protection laws and industry standards; and
>
> 6. Reviewing our privacy and data governance programs.

Based on the detailed knowledge of cybersecurity threats, risks, controls, and compliance that is needed to undertake these tasks, we conclude that it would be highly challenging for a committee with no members having cybersecurity education, work experience, or certifications/training to adequately complete them. Indeed, such a situation could contribute to missed vulnerability identification or compliance oversights.

On the other hand, a case could be made that experts are not strictly necessary and that directors with cybersecurity literacy, alongside a business and risk management background, may be sufficient (Lowry et al., 2021). In cases where deep cybersecurity skills are required for a particular board task, external specialists/consultants could be brought in to provide specific advice (Vincent et al., 2019; Wang et al., 2023). Other commentators have recognized that some cybersecurity experts may have limited familiarity with general management, governance, and strategic issues, which may limit their contributions on other board topics (Czarnecki, 2015; IANS, 2023). As well, having a cybersecurity expert on the board may encourage other directors to become complacent and defer responsibility to the expert rather than voicing their own opinions on the topic (PwC, 2024).

[3] Our data shows that 89.6% of directors serving on the cybersecurity committee also serve on other board committees.

Despite these counterarguments, we question their applicability in the context of a narrowly focused cybersecurity committee. That is, when the committee's focus is fully oriented toward cybersecurity issues, we see no tangible benefit arising from having no members with domain-specific expertise. However, it is plausible that an optimal cybersecurity committee is one that is neither entirely filled with highly technical domain experts nor one that has no expert members whatsoever, but rather is composed of a balance of cybersecurity, business, and risk expertise.

Recommendations

Based on our findings, we make the following recommendations, targeted toward the board of directors.

Board Recommendation #1: Set minimum cybersecurity expertise/literacy requirements for cybersecurity committee members. We suggest that all members of a cybersecurity committee should have attained a basic level of literacy on cybersecurity issues and at least one member of the committee should have cybersecurity expertise. Board members should take advantage of risk and governance-oriented programs, such as those offered by the National Association of Corporate Directors to fulfill the necessary criteria.

Recommendation #2: Leverage non-traditional sources to identify potential cybersecurity committee members. Boards need to move beyond their continued reliance on networks of senior business executives and existing board members to identify cybersecurity experts who are suitable for board positions. We suggest that considering non-traditional sources, such as those serving in senior roles in professional services firms (e.g., Big-4 accounting), business school academics, and leaders in cybersecurity firms can provide a rich source of cybersecurity expertise, alongside the necessary business and communication skills.

Recommendation #3: Clarify to stakeholders why a cybersecurity committee provides more effective oversight than alternative structures. Although the creation of a cybersecurity committee signals to stakeholders that the board recognizes the importance of the area, the board should be transparent in demonstrating the specific benefits of a cybersecurity-specific committee, which could include more frequent meetings with management, more in-depth oversight activities, and/or the opportunity to appoint more narrowly focused experts to the board. Convincing stakeholders that the board is more "cyber warrior" than "cyber washing" by appointing domain experts to the cybersecurity committee will go a long way to advance trust in their corporate governance capabilities.

Limitations and future research

As with any research, this study is subject to several limitations, alongside opportunities for future research. First, since our focus was strictly on board-level cybersecurity committees, our findings pertaining to director expertise levels will not necessarily apply to other committees responsible for cybersecurity governance (e.g., the audit committee) or to the board of directors in general. Second, we acknowledge that judgments on an individual's level of expertise are subject to change. As such, the data we collected on individual directors was collected at the time of the study, but it is possible that the directors subsequently undertook activities, such as completing training programs, that would influence our assessment of their expertise. It is also possible that some directors did have cybersecurity education, experience, and/or training, but that this information was not publicly available. Similarly, it is possible that some directors had indirect experience or exposure to cybersecurity and technology that was not apparent in the sources available to us. For example, a CFO at an internet software company or a director who sits on multiple boards of technology companies might not have direct cybersecurity experience but could well exceed the bar of being cybersecurity literate. As such, it is possible that cybersecurity expertise could be underreported in some instances. Finally, we note that there are many cybersecurity training and certification options available to practitioners that vary widely in their breadth, intensity, and time commitment. Although we group these educational activities together for simplicity in our evaluation of expertise, we acknowledge a quote from a practitioner who argued in a recent article that "you can't substitute somebody's cyber experience and knowledge from a lifetime of professional experience into a two-week course. So, sending board directors to this type of training and saying they're experts can be misleading" (Chickowski, 2023). As such, we encourage care in labeling a director as being an expert based only on the completion of a week-long cybersecurity course (in comparison to completing a course and also having cybersecurity work experience, for example).

Several opportunities for future research stem from this study. First, we encourage qualitative, case-based investigations that compare how cybersecurity committee "generalists" perform in meetings relative to

those with expert-level education, training, and experience. Past research (e.g., Ericsson & Smith, 1991) advocates for expert-novice comparisons in order to clearly articulate what expertise represents in a particular domain. Second, future research could further examine the signaling theory aspect of our study by investigating the market's reaction (e.g., share price) to a firm's announcement of the creation of a cybersecurity committee. In relation to the findings of our study, it would be particularly interesting to see if the reaction is different when a firm simply announces the formation of such a committee compared to a committee announcement alongside the names and credentials of a robust team of cybersecurity expert committee members.

Conclusion

This work draws on the expertise and corporate governance literature to evaluate the suitability of board members serving on a firm's cybersecurity committee based on domain-specific education, experience, and training. Our results reveal a startlingly low level of cybersecurity-specific expertise, partly offset by relatively robust technology and general business backgrounds. In revealing the disconnect between firms that establish cybersecurity committees, but then fail to nominate board members with domain-specific expertise, we question the incremental benefit of the cybersecurity committee, relative to existing governance structures. We call on boards to not only "talk the talk" but also "walk the walk" when addressing cybersecurity risks by appointing at least one domain expert to their cybersecurity committee. We provide a series of recommendations to help advance this goal.

References

Abraham, C., O'Connell, S. C., Giuffrida, I., & Sims, R. R. (2024). Adding cybersecurity expertise to your board. MIT Sloan Management Review, 65(2), 1-6.

Adams, R. B., Hermalin, B. E., & Weisbach, M. S. (2010). The role of boards of directors in corporate governance: A conceptual framework and survey. Journal of Economic Literature, 48(1), 58-107.

Bandodkar, N. R., & Grover, V. (2022). Does it pay to have CIOs on the board? Creating value by appointing C-level IT executives to the board of directors. Journal for the Association for Information Systems, 23(4), 838-888.

Baysinger, B. D., & Butler, H. N. (2019). Corporate governance and the board of directors: Performance effects of changes in board composition. In R. I. Tricker (Ed.), Corporate governance (pp. 101-124). Gower.

Bédard, J., & Gendron, Y. (2010). Strengthening the financial reporting system: Can audit committees deliver? International Journal of Auditing, 14, 174-210.

Bill Holdings Inc. (2023). Schedule 14a - proxy statement. https://www.sec.gov/Archives/edgar/data/1786352/000114036123049688/ny20010024x1_def14a.htm

Boivie, S., Withers, M. C., Graffin, S. D., & Corley, K. G. (2021). Corporate directors' implicit theories of the roles and duties of boards. Strategic Management Journal, 42(9), 1662-1695.

Caluwe, L., & De Haes, S. (2019). Board engagement in IT governance: Opening up the black box of IT oversight committees at board level. Proceedings of the 52nd Hawaii International Conference on System Sciences, Wailea, HI.

Camerer, C. F., & Johnson, E. J. (1991). The process-performance paradox in expert judgement. In K. A. Ericsson & J. Smith (Eds.), Toward a general theory of expertise (pp. 195-217). Cambridge University Press.

Center for Audit Quality. (2023). 2023 audit committee transparency barometer. https://thecaqprod.wpenginepowered.com.

Chase, W. G., & Simon, H. A. (1973). The mind's eye in chess. In W. G. Chase (Ed.), Visual information processing (pp. 215-281). Academic Press.

Chen, K. D., & Wu, A. (2016). The structure of board committees. https://www.hbs.edu.

Chickowski, E. (2023). How much cybersecurity expertise does a board need? CSO. https://www.csoonline.com/article/656596/how-much-cybersecurity-expertise-does-a-board-need.html

Connelly, B. L., Certo, S. T., Ireland, R. D., & Reutzel, C. R. (2011). Signaling theory: A review and assessment. Journal of Management, 37(1), 39-67.

Couchoux, O. (2024). Navigating knowledge and ignorance in the boardroom: A study of audit committee members' oversight styles. Contemporary Accounting Research, 41(1), 459-497.

Czarnecki, G. M. (2015). Cyber threats necessitate a new governance model. NACD Directorship(September), 7-9.

Defond, M. L., Hann, R. N., & Hu, X. (2005). Does the market value financial expertise on audit committees of boards of directors? Journal of Accounting Research, 43(2), 153-193.

Deiso, P. (2022). Cybersecurity and climate risk: Does your board need an expert? RSM. https://rsmcanada.com.

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

DeMayo, T., & DeLena, N. (2024). Five critical cybersecurity considerations for 2024. Directors & Boards. https://www.directorsandboards.com.
Ericsson, K. A., & Charness, N. (1994). Expert performance: Its structure and acquisition. American Psychologist, 49(8), 725-747.
Ericsson, K. A., & Smith, J. (1991). Prospects and limits of the empirical study of expertise: An introduction. In K. A. Ericsson & J. Smith (Eds.), Toward a general theory of expertise (pp. 1-38). Cambridge University Press.
Ferracone, R. (2019). Good governance: Do boards need cyber security experts? Forbes. https://www.forbes.com.
Forrest, W., Li, S., Tamburro, I., & Van Kuiken, S. (2022). How effective boards approach technology governance. McKinsey Digital. https://www.mckinsey.com.
Free, C., Trotman, A. J., & Trotman, K. T. (2021). How audit committee chairs address information-processing barriers. The Accounting Review, 96(1), 147-169.
Garb, H. N. (1989). Clinical judgement, clinical training, and professional experience. Psychological Bulletin, 105(3), 387-396.
Héroux, S., & Fortin, A. (2024). Board of directors' attributes and aspects of cybersecurity disclosure. Journal of Management and Governance, 28, 359-404.
Higgs, J. L., Pinsker, R. E., Smith, T. J., & Young, G. R. (2016). The relationship between board-level technology committees and reported security breaches. Journal of Information Systems, 30(3), 79-98.
Hitchcock, C., Lamm, B., & Parsons, K. (2017). On the board's agenda: U.S. Trends in audit committee reporting. Deloitte. https://www2.deloitte.com.
IANS. (2023). CISOs as board directors: CISO board readiness analysis. https://cdn.iansresearch.com/Files/Marketing/CISOsasBoardDirectors-CISORecommendations.pdf
Jewer, J., & McKay, K. (2012). Antecedents and consequences of board IT governance: Institutional and strategic choice perspective. Journal of the Association for Information Systems, 13(7), 581-617.
Lanz, J. (2014). Cybersecurity governance. The CPA Journal, 84(11), 6-10.
Larcker, D. F., Reiss, P. C., & Tayan, B. (2017). Critical update needed: Cybersecurity expertise in the boardroom. SSRN. https://ssrn.com/abstract=3074594
Lowry, M., Vance, A., & Vance, M. D. (2021). Inexpert supervision: Field evidence on boards' oversight of cybersecurity. SSRN.
McDaniel, L., Martin, R. D., & Maines, L. A. (2002). Evaluating financial reporting quality: The effects of financial expertise vs. Financial literacy. The Accounting Review, 77, 139-167.
Milică, L., & Pearlson, K. (2023). Boards are having the wrong conversations about cybersecurity. Harvard Business Review. https://hbr.org/2023/05/boards-are-having-the-wrong-conversations-about-cybersecurity
Nash, K. S. (2023). Cyber chiefs seeking board seats have their work cut out for them. Wall Street Journal. https://www.wsj.com/articles/cyber-chiefs-seeking-board-seats-have-their-work-cut-out-for-them-69856922
NightDragon. (2023). State of cyber awareness in the board room report. https://www.nightdragon.com/wp-content/uploads/State-of-Cyber-Awareness-in-the-Board-Room-Report.pdf
Nolan, R., & McFarlan, F. W. (2005). Information technology and the board of directors. Harvard Business Review, 83(10), 96-106.
O'Donnell-Welch, I. (2023). More companies adopt board-level cybersecurity committees. Duo Security. https://duo.com/decipher/more-companies-consider-board-level-cybersecurity-committees
Premuroso, R. F., & Bhattacharya, S. (2007). Is there a relationship between firm performance, corporate governance, and a firm's decision to form a technology committee? Corporate Governace, 15(6), 1260-1276.
Price, J. B., & Lankton, N. (2018). A framework and guidelines for assessing and developing board-level information technology committee charters. Journal of Information Systems, 32(1), 109-129.
Proudfoot, J. G., Cram, W. A., Madnick, S., & Coden, M. (2023). The importance of board member actions for cybersecurity governance and risk management. MIS Quarterly Executive, 22(4), 235-250.
PwC. (2023). Board effectiveness: A survey of the c-suite. https://www.pwc.com/us/en/services/governance-insights-center/library/board-effectiveness-and-performance-improvement.html
PwC. (2024). Overseeing cyber risk: The board's role. https://www.pwc.com/us/en/services/governance-insights-center/library/assets/pwc-gic-overseeing-cyber-risk-v2.pdf
U.S. Securities and Exchange Commission. (2023). Cybersecurity risk management, strategy, governance, and incident disclosure. https://www.sec.gov/files/rules/final/2023/33-11216.pdf
Vasileiou, I., & Furnell, S. (2018). Enhancing security education: Recognising threshold concepts and other influencing factors. Proceedings of the 4th International Conference on Information Systems Security and Privacy, Portugal.
Vincent, N. E., Higgs, J. L., & Pinsker, R. E. (2019). Board and management-level factors affecting the maturity of IT risk management practices. Journal of Information Systems, 33(3), 117-135.
Violino, B. (2023). Cybersecurity experts have become targets for board seats. CNBC. https://www.cnbc.com/2023/07/03/cybersecurity-experts-have-become-targets-for-board-seats.html
Wang, Q., Ngai, E. W. T., Pienta, D., & Thatcher, J. B. (2023). Information technology innovativeness and data-breach risk: A longitudinal study. Journal of Management Information Systems, 40(4), 1139-1170.
Wu, Y., Zhang, K., & Xie, J. (2020). Bad greenwashing, good greenwashing: Corporate social responsibility and information transparency. Management Science, 66(7), 3095-3112.