Inexpert Supervision:

Field Evidence on Boards' Oversight of Cybersecurity

Abstract

We conduct a field study of boards' emerging responsibility to oversee cybersecurity risk, a setting in which few directors have expertise. We find that although nonexpert directors may genuinely seek to provide substantive oversight, without expertise their efforts lack effectiveness and therefore serve an essentially symbolic function, even when they perform the same oversight activities as expert directors. We also explore why boards do not prioritize appointing cybersecurity experts and show that nonexpert directors do not perceive that their efforts are symbolic and insufficient. In contrast, expert directors perceive keenly the deficiency of their nonexpert counterparts and argue for the need for more cybersecurity experts on boards, and this viewpoint is shared by cybersecurity executives and consultants who support the board. Thus, we contribute to our understanding of when boards are likely to provide substantive versus symbolic oversight and inform the debate on the need for board-level cybersecurity expertise.

Keywords: corporate governance, boards of directors, board oversight, risk oversight, cybersecurity risk, agency theory, institutional theory, expertise, boundary condition, qualitative field study.

Inexpert Supervision: Field Evidence on Boards' Oversight of Cybersecurity

The cyber threat is a corporate governance issue. The companies that handle it best will have relevant expertise in the boardroom…

SEC Commissioner Robert Jackson, 2018

[M]ost boards are simply completely incapable of overseeing cyber risk. It's just so far outside of their experience and their expertise that all they can do is assess the credibility of the executives that are put in front of them.

Former NASDAQ Board Director

1. Introduction

Cybersecurity[1] is increasingly viewed by boards of directors, investors, and regulators as a key enterprise risk, and corporate boards are under growing pressure to appropriately oversee this risk (PwC 2022, Milica and Pearlson 2023). For example, in 2023 the SEC introduced a new regulation requiring public companies to describe in their annual reports "the board of directors' oversight of risks from cybersecurity threats" (SEC 2023, p. 171). However, a persistent concern is whether boards of directors have sufficient expertise to oversee cybersecurity risk (SEC 2022). An analysis of the S&P 500 found that only 12 percent of boards had a director with cybersecurity expertise (Rundle 2023). Similarly, we analyzed 1,000 randomly selected proxy statements from among the Russell 3000 and found that fewer than 15% of firms disclose having any director with cybersecurity expertise (by contrast, 100 percent of firms disclosed having financial experts on their boards).[2] Emphasizing the importance of this issue, in 2023 the New York State Department of Financial Services (NYDFS) issued rules requiring boards to have "sufficient understanding of cybersecurity-related matters to exercise [cybersecurity] oversight" (NYDFS 2023, p. 7).

The context of cybersecurity oversight brings into relief a lack of understanding in the corporate governance literature with respect to boards' performance of substantive versus symbolic oversight. Agency theory emphasizes independent and substantive monitoring, while institutional theory argues that boards are motivated to adopt legitimate oversight behaviors that can take on a ceremonial character. However,

[1] The SEC defines cybersecurity as "The body of technologies, processes and practices designed to protect networks, systems, computers, programs and data from attack, damage or unauthorized access" (SEC 2011).

[2] We conducted this analysis in 2020 using the 2019 Russell 3000, as a sensitizing background analysis at the commencement of our study.

prior research provides evidence that neither theory fully explains oversight practices, and that boards display a mix of both substantive and symbolic oversight (e.g., Kalbers and Fogarty 1998; Beasley, Carcello, Hermanson, and Neal 2009; Cohen, Krishnamoorthy and Wright 2010; Clune, Hermanson, Tompkins, and Ye 2014; Trotman and Trotman 2015; Couchoux 2023). Moreover, prior research has generally examined boards' substantive versus symbolic oversight of well-established board responsibilities for which board-level expertise is common. In contrast, the role of expertise in the oversight of emerging risk areas, for which board expertise is scarce, is an open question.

We examine how domain expertise influences directors' activities and effectiveness in the novel context of cybersecurity risk oversight. On one hand, because cybersecurity is widely acknowledged by investors, regulators, and directors themselves as a key enterprise risk, we expect to see boards conduct independent and substantive monitoring of this emerging risk. On the other hand, board cybersecurity expertise remains uncommon (Cheng et al. 2021). This lack of expertise plausibly increases boards' uncertainty about cybersecurity oversight, and institutional theory suggests that boards respond to uncertainty by conforming to isomorphic pressures and performing legitimate practices which may or may not lead to the end goal of effective oversight. If legitimate practices do not constitute substantive oversight (e.g., because the directors performing them lack sufficient expertise), such oversight is considered symbolic even if not intentionally meant to be. Therefore, cybersecurity risk oversight provides an important context for examining the influence of expertise on boards' performance of substantive versus symbolic oversight. Specifically, we address the following research question:

RQ: *How does cybersecurity expertise influence directors' substantive or symbolic oversight behaviors?*

To investigate this question, we performed a qualitative field study, using methods well suited to gaining in-depth insight into boards' monitoring activities and decision-making (Yin 2018), and which have been used in recent accounting research (e.g., Bills, Hayne, and Stein 2018; Hayne and Vance 2019; Dodgson, Agoglia, Bennet, and Cohen 2020). We conducted interviews with 20 board directors, both with and without cybersecurity expertise, about how expertise influences boards' cybersecurity oversight.

Furthermore, because our research question involves the nature of the oversight provided, we also interviewed 18 cybersecurity experts—executives and senior-level consultants—who support boards of directors. In this way, we corroborated the perspectives of expert directors with those of executives and consultants with bona fide cybersecurity expertise.

Our analysis demonstrates that cybersecurity expertise is an important factor in determining the substantive versus symbolic nature of boards' oversight behaviors. We find that there is a clear consensus among our participants that cybersecurity risk is a top priority, and thus directors seek guidance on legitimate oversight practices from regulators, industry groups, and peer firms. However, we conclude that these oversight practices often lack substance and independence when performed by board members with low cybersecurity expertise. For example, an emerging best practice entails using board meeting time to receive cybersecurity reports and ask questions of cybersecurity executives. Our participants shared that when nonexpert boards engage with cybersecurity executives, they often ask superficial questions (such as "How are we doing?") or reactive questions (such as "Could that happen to us?" in response to a cyber incident in the media). Further, inconsistent with independent monitoring under agency theory, several participants shared that a lack of cybersecurity expertise leads some 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.[3] Without expertise, directors are less likely to perceive CISOs obfuscating damaging information about the firm's cybersecurity position as an issue and are less able to detect when CISOs filter reports to inflate directors' assessment of executives' cybersecurity performance, and their oversight of cybersecurity risk generally lacks independence.

Given our observation that board-level expertise is relatively uncommon, as well as our findings that cybersecurity expertise is needed for substantive oversight, we also explore why boards do not appear to prioritize the appointment of cybersecurity experts. Most of our interviewees emphasized practical

[3] For ease of exposition, we refer to senior executives with direct responsibility over cybersecurity collectively as "CISOs". These are typically executives that are embedded in the executive suite two or more layers from the CEO, most often through the Chief Information Officer.

constraints, such as the scarcity of expertise in the director labor market and the recency of cybersecurity's emergence as a top risk. However, our analysis suggests a more fundamental reason for boards not appointing cybersecurity experts: nonexpert directors believe they are able to provide adequate oversight despite not having cybersecurity expertise due to their general business and oversight experience, coupled with following legitimate best practices. In contrast, expert directors perceive a clear improvement in oversight effectiveness when boards have genuine cybersecurity expertise, and this view is corroborated by CISOs and consultants. Overall, we conclude that when boards have cybersecurity expertise, they provide substantive oversight, as predicted by agency theory. In contrast, in the absence of expertise, boards seek legitimacy by following best practices, consistent with institutional theory. However, without expertise these practices lack effectiveness and thus constitute primarily ceremonial oversight. This is the case even when expert and nonexpert directors conduct similar oversight activities.

We answer research calls to better understand the "differences in the form and substance of corporate governance" (Cohen et al. 2008a, p. 40) as well as the board characteristics and activities that lead to differential oversight effectiveness (Cheng et al. 2021). Our analysis suggests that low expertise increases the board's uncertainty regarding both underlying cybersecurity risk and related oversight tasks, such that boards tend toward isomorphism by adopting legitimate but essentially symbolic oversight actions. Prior research argues that boards intentionally engage in symbolic oversight "to convey to *external parties* that the trappings of governance are in place" (Cohen, Krishnamoorthy and Wright 2008b, 194, emphasis added). We enrich this theory by showing that nonexpert directors perform ritualistic activities because they *themselves* believe that these activities are legitimate and effective. Further, prior field studies conclude that uncooperative but powerful management contributes to boards providing symbolic oversight (Beasley et al. 2009, Cohen et al. 2010, Hermanson et al. 2012). In our setting, CISOs are not considered to be powerful relative to board members or the C-suite (Lowry et al. 2022); hence, we find that low expertise is a novel reason board members over-rely on and defer to management.

We also contribute to the debate on the need for cybersecurity expertise on the board (Larcker et al. 2017, Ferracone 2019). We believe our findings can provide useful inputs into regulators' and market

participants' board composition decisions relative to cybersecurity expertise. Cybersecurity risk governance and disclosure continue to be a high priority for SEC rulemaking (SEC 2021c, 2021a, 2021d, 2021b, 2022, 2023). Further, in their proposed rule, the SEC asserts that directors' cybersecurity expertise is relevant to investors (SEC 2022). While the importance of board financial expertise is well established in the literature, the SEC's proposal to require cybersecurity expertise disclosures similar to those required for financial expertise has been met with controversy[4] and was eventually removed in its final rule (SEC 2023). Moreover, given that the majority of public company boards do not have a cybersecurity expert , this suggests that the need for expertise in this domain remains an open question. While addressing the optimal level of board cybersecurity expertise is outside the scope of our analysis, we provide field evidence showing that in the absence of expertise, boards are more likely to provide symbolic oversight and may rely excessively on management such that the terms of oversight (e.g., reporting content, objectives, and performance metrics) are largely dictated by the executives who are supposed to be the subjects of that oversight. Such circular governance appears unlikely to effectively mitigate agency conflicts and may potentially expose firms to increased risk of cybersecurity failure.

Although our focus is on boards' oversight of cybersecurity, we also contribute to the broader corporate governance literature examining the influence of directors' domain expertise on related outcomes (e.g., McDaniel, Martin, and Maines 2002; Agrawal and Chadha 2005; Fich and Shivdasani 2007; Cohen et al. 2014; Baugh, Hallman, and Kachelmeier 2021). While prior archival studies demonstrate that expertise is related to oversight outcomes, we complement these studies by opening the "black box" of board oversight, providing rich narrative examples of how directors respond to an emerging oversight responsibility. A few qualitative studies indicate expertise may matter for the nature of oversight but leave several issues unaddressed. For instance, Beasley et al. (2009) find that directors with accounting expertise carefully vet their board positions so as to work with top executives that are agreeable to monitoring, but do not explore whether differences in oversight behaviors extend beyond this selection effect. Likewise,

[4] As discussed in Section 2, an analysis of SEC comment letters finds that comments against the disclosure rule outnumber those in favor nearly two to one.

Cohen et al. (2010) discuss audit committee members' financial expertise and power interchangeably, suggesting that perhaps expertise confers power; however, they do not directly assess how expertise affects oversight behaviors. We extend the findings of this past research by showing how expertise affects a range of oversight activities.

Moreover, our study of the role of expertise in the context of an emerging board responsibility where expertise is scarce is important given that the prior research has focused on financial reporting oversight (e.g., Couchoux 2023, Cohen et al. 2010, Beasley et al. 2009). For instance, Couchoux (2023) finds that audit committee members' within–board relative expertise influences their "style," or the oversight roles they choose to take on. However, while all audit committee members in Couchoux's setting are either financially literate or expert, for an emerging board responsibility setting like cybersecurity, expertise is the exception rather than the rule. Thus, while Couchoux's (2023) focus is on how audit committee members self-select complementary roles based on their relative expertise, our focus is on how boards oversee risks for which individual and collective expertise is sparse. Given that specific responsibility for cybersecurity oversight is often placed on audit committees (Center for Audit Quality and Deloitte 2022), and financial experts are rarely also cybersecurity experts, our findings provide timely feedback to audit committees on one of their emerging responsibilities.

2. Background and Related Theory

2.1.Background

Cybersecurity incidents are increasingly prevalent and result in trillions of dollars in estimated losses annually (Fox 2021). The negative consequences of cybersecurity incidents include interruptions to operations, reputational costs, worse loan terms, and loss of firm market value (Huang and Wang 2021, Kamiya et al. 2021, Tidy 2021, Tunggal 2021). Consequently, cybersecurity risk management is increasingly viewed as critical to firms' success (Doan 2019, KPMG 2021), with firms spending over $150 billion annually on cybersecurity, a figure projected to increase to well over $200 billion by 2025 (Gartner

2021).[5] However, experts believe these financial investments are often in the wrong security initiatives, underscoring the need for boards to oversee cybersecurity investments to ensure that they provide value to shareholders (Morgan 2019; ISA and NACD 2020) .

Reflecting these trends and concerns, there have been numerous calls for board-level oversight of cybersecurity risks. For example, the Council of Institutional Investors (CII) states that "[e]ffective cybersecurity risk management starts with the board" (CII 2016, 2), and the Federal Trade Commission (FTC) asserts that "data security begins with the Board of Directors, not the IT Department" (FTC 2021). In some cases, federal and state regulations already specifically mandate that boards oversee cybersecurity. For example, since 2001, the U.S. Treasury's Office of the Comptroller of the Currency (OCC) has required boards to "[o]versee the development, implementation, and maintenance of the bank's information security program…" and to receive related cybersecurity reports from management at least annually (66 FR 8633).[6] The NYDFS issued similar rules for financial services firms operating in New York (s 500.4[b] 2017). This same regulation has since become law for licensed insurance companies in more than a dozen states (Blosfield 2021) and it is likely that regulators of other industries will adopt rules such as those of the OCC and NYDFS in the future (PwC 2021), as the FTC has done with its 2023 amendments to its Safeguards Rule governing financial institutions (FTC 2022). As noted previously, the NYDFS rules were also updated in 2023 to require additional specific oversight actions from boards of directors, such as annually approving the cybersecurity plan and receiving timely reports of significant cybersecurity incidents from the CISO (NYDFS 2023).

Moreover, oversight of cybersecurity has been a point of emphasis for the SEC since at least 2011 (SEC 2011), with Commissioner Robert Jackson calling the rising cyber threat "the most pressing issue in corporate governance today" (Jackson 2018) and Commissioner Luis Aguilar cautioning that "boards that

[5] A recent survey conducted by RBC Global Asset Management found cybersecurity to be institutional investors' top concern among environmental, social, and governance (ESG) issues (RBC 2019).
[6] Notably, the OCC specifically cited the failure of Capital One's board to provide effective cybersecurity oversight as a key reason for levying an $80 million fine in connection with Capital One's 2019 data breach (U.S. Department of the Treasury 2020).

choose to ignore, or minimize, the importance of cybersecurity oversight responsibility, do so at their own peril" (Aguilar 2014). Accordingly, the SEC's 2023 rule requires that boards explain their oversight of cybersecurity threats and whether the board directly receives reports from the CISO (SEC 2023).

Despite the urgency of effective cybersecurity programs and the expectations for directors to oversee them, survey evidence suggests that directors do not have sufficient expertise to provide adequate oversight of cybersecurity risk (NACD 2018). For example, in their survey of 577 U.S. public company directors, Cheng et al. (2021) find that directors perceive cybersecurity to have the *lowest* level of board effectiveness among the 19 responsibility areas considered, which the authors attribute to limited board-level experience or expertise. This may be because audit committees, whose primary tasks involve financial reporting oversight, are often the primary providers of cybersecurity risk oversight (Center for Audit Quality and Deloitte 2022).

To address this apparent expertise gap, the SEC proposed rules that would require public companies to disclose whether they have a director with cybersecurity expertise (SEC 2022). However, this proposed rule was met with controversy, as many market participants viewed the rule as a de facto mandate for board-level cybersecurity (e.g., following the adoption of similar rules regarding financial expertise under SOX, all public company boards now have a financial expert), which they do not believe is practical or needed. To assess the tension and debate around the need for board cybersecurity expertise, we analyzed SEC comment letters and find that 83 specifically address the proposed board expertise rule (other letters focus on issues related to cybersecurity disclosure more broadly). Of these, 27 are in favor of the rule, 48 are against the rule, and eight present mixed views. Proponents of the rule assert that cybersecurity expertise is needed to provide adequate oversight. Those against the rule point to a scarcity of cybersecurity experts who are also qualified to be board members and claim that domain expertise is not needed for directors to sufficiently perform their fiduciary requirements for risk oversight.[7] Ultimately, in 2023 the SEC released

[7]Appendix B provides details of our analysis of SEC comment letters and includes representative quotes both in favor and against the proposed rule.

its final rules wherein cybersecurity oversight was emphasized but the requirement to disclose director cybersecurity expertise was removed.

2.2.Theoretical Lenses

We follow Malsch and Salterio's (2016) suggestions for the use of theory in positivist field research. First, we consider investors' and regulators' expectations and standards discussed above as normative theory (Malsch and Salterio 2016), which serves as a baseline against which practices observed in the field can be evaluated. Second, we use theories from related disciplines to form expectations against which to compare our findings. Agency theory (e.g., Jensen and Meckling 1976; Fama and Jensen 1983; Eisenhardt 1989) is the dominant lens through which corporate governance is viewed in the accounting and finance literatures (Beasley et al. 2009), particularly as it relates to boards' monitoring (as opposed to advising) role.[8] Therefore, we use an agency perspective as a starting point from which to develop expectations for how boards will respond to their emerging cybersecurity oversight responsibilities. We also incorporate perspectives from institutional theory to generate potential alternative predictions.

Prior studies show that boards exhibit a range of oversight postures, from substantive to symbolic. Some suggested reasons for boards providing symbolic oversight include management attitude (i.e., willingness to be subject to oversight) coupled with management power (Beasley et al. 2009, Cohen et al. 2010, Hermanson et al. 2012) and management-director social ties (Hwang and Kim 2009, Bruynseels and Cardinaels 2014). On the other hand, substantive oversight is more likely after governance-related regulation (Cohen et al. 2010) and when directors have greater reputational concerns (Masulis and Mobbs 2014, Sila et al. 2017). While expertise has been cited as a potential differentiator, it has been conflated with director–management power dynamics (Cohen et al. 2010).[9] Although audit committees largely

[8] Broadly, boards of directors play both a monitoring and an advising role (e.g., Faleye , Hoitash, and Hoitash 2011), and agency theory and resource dependence theory have traditionally served as the primary lens for the former and latter, respectively (Hillman and Dalziel 2003). While acknowledging directors' advising role, we focus in this paper on monitoring, consistent with the SEC's guidance emphasizing board's cybersecurity oversight responsibilities.

[9] Cohen et al. (2002) examine auditors' experiences with audit committees and find that audit committees are often passive; while they conjecture low expertise may be one reason for this passivity, their study focuses on the role management plays in corporate governance and issues with audit committee power and independence. Cohen et al.

exhibit substantive oversight over financial reporting (Beasley et al. 2009, Cohen et al. 2010), there is evidence that audit committees exhibit more symbolic oversight over their other duties, such as ERM (Cohen et al. 2017) or environmental reporting (Trotman and Trotman 2015); however, these studies do not connect symbolic oversight to a lack of expertise. Next, we discuss theoretical expectations for why director expertise may influence the substantive versus symbolic nature of oversight.

2.3.Agency Theory Perspective

Management is responsible for assessing and managing firm risk. From an agency perspective, top managers may not act in the best interests of shareholders due to insufficient ability or conflicting preferences (or both). For example, a CISO may prefer to shirk rather than incur personal cost from effort or may select inefficient cybersecurity investments that do not adequately mitigate risk. A fundamental tenet of agency theory is that shareholders seek to mitigate agency costs by separating decision management from decision control, and the board of directors serves as the apex of the decision control system (Fama and Jensen 1983, 323). Due to the potential for conflicts (and resulting costs) between shareholders and managers, agency theory suggests that the board's "most important role is to scrutinize the highest decision makers within the firm" (Fama 1980, 294). Hence, agency theory predicts that directors will be diligent monitors of material firm risks and executives over those risks, including cybersecurity risks.

The agency perspective of corporate governance broadly assumes that the board possesses sufficient general monitoring expertise to provide an independent[10] check on management (e.g., Fama and Jensen 1983). However, domain-specific expertise is increasingly recognized as important for boards to fulfil their intended monitoring role (Hillman and Dalziel 2003, Hambrick et al. 2015). While there is limited existing

(2010) updated their 2002 study and find audit committees to be more active post-SOX, citing higher independence, power, and expertise. Neither of the Cohen et al. studies focused on the effect of expertise on oversight behaviors per se. They instead emphasized power dynamics and stopped short of discussing the role of expertise itself on oversight behavior, suggesting that expertise is part of the mix of desirable attributes for audit committees.

[10] While the governance implications of director independence are well studied in the prior literature, much of this research focuses on structural independence, which is typically measured as whether directors have a primary employment relationship with the firm or otherwise have preexisting relationships with the executive team (e.g., Weisbach 1988; Beasley 1996; Klein 2002; Chen et al. 2015). More fundamentally, however, independence relates to a director's ability to form their own assessment of the firm's risks, programs, and performance apart from assessments as provided by the management team (Hambrick et al. 2015).

research on the importance of cybersecurity expertise for oversight effectiveness, related literature on financial expertise emphasizes that expertise enhances monitoring. For example, studies have shown that financial expertise is positively associated with financial reporting quality and related outcomes (McDaniel et al. 2002, Xie et al. 2003, Abbott et al. 2004, Bédard et al. 2004, Agrawal and Chadha 2005, Krishnan 2005, Goh 2009, Hoitash et al. 2009, Lisic et al. 2019), and that market participants react favorably when a financial expert is appointed to the audit committee (DeFond et al. 2005).[11] As with financial reporting, cybersecurity is a technical domain; thus, boards' oversight of their firms' cybersecurity programs may similarly benefit from (or even necessitate) domain-specific expertise. Therefore, based on agency theory, we expect boards to have or seek adequate expertise to provide independent, effective oversight.

2.4.Institutional Theory Perspective

Institutional theory is sometimes positioned as a perspective that competes with agency theory, as its predictions for board oversight contrast heavily (e.g., Beasley et al. 2009; Cohen et al. 2010; Hermanson et al. 2012). Institutional theory predicts that board practices reflect pressures to appear legitimate (DiMaggio and Powell 1983). Legitimacy is defined as the "generalized perception or assumption that the actions of an entity are desirable, proper, or appropriate within some socially constructed system of norms, values, beliefs, and definitions" (Suchman 1995, p. 574). Legitimate behavior emerges as part of an organizational convergence process (Holder-Webb et al. 2009), formally called "isomorphism" under institutional theory. For example, firms look toward regulatory guidance (such as the SEC or NYDFS) under coercive isomorphism, toward peers (such as networks of board members) under mimetic isomorphism and toward professional groups (such as the NACD) under normative isomorphism. In contrast to agency theory, which emphasizes a board's substantive oversight, institutional theory suggests the board's goal is perceived legitimacy of their oversight practices, and that such practices may consist of symbolic rather than substantive oversight (Cohen et al. 2010, Bromley and Powell 2012, Wijen 2014).

[11] Beyond financial expertise, studies show that director expertise improves board effectiveness in matters related to the legal (Krishnan et al. 2011), human resources (Mullins 2018), and technology domains (Ashraf et al. 2020).

DiMaggio and Powell (1983) posit that a driving force behind isomorphism is uncertainty about "organizational technologies," or processes and practices. Specifically, institutional theory predicts that firms will exhibit institutional isomorphism for the sake of legitimacy when there is uncertainty about the relationship between means and ends, or when there is uncertainty about the goals of organizational practices and processes (DiMaggio and Powell 1983). For example, in the face of uncertainty, firms will mimic the governance behaviors of "leading" organizations for the sake of legitimacy (Cohen et al. 2008b), which may or may not result in effective oversight. While early interpretations of symbolic action under institutional pressures was framed as a decoupling of policy and practice (symbolic adoption), in opaque institutional fields, such as cybersecurity oversight, a more relevant phenomenon is a decoupling of means and ends (Bromley and Powell 2012, Wijen 2014). That is, under institutional theory, some board practices may be legitimate without substantively improving oversight. For example, board questioning of executives may be the appropriate means (legitimate oversight behaviors), but if questioning is superficial, it will likely not result in the desired end (meaningful oversight outcomes). Further, this decoupling may happen due to the uncertainty of cybersecurity instead of self-interested intent (Wijen 2014). Given the evolution of cybersecurity risk itself, as well as the nascency of cybersecurity risk oversight as a key board responsibility, we expect that ambiguity about organizational cybersecurity goals and uncertainty about best practices is likely to be especially prevalent in our setting.

Further, we expect that directors' expertise in the cybersecurity domain (rather than monitoring expertise generally) is an important factor for a director's uncertainty about the relationship between cybersecurity means and ends, wherein low expertise increases uncertainty about both cybersecurity risk itself, and about its oversight. Therefore, based on institutional theory, we may expect boards with low expertise to respond to their emerging responsibility to oversee cybersecurity by performing oversight actions based on isomorphic pressures. Such oversight actions may appear legitimate, but ultimately represent symbolic oversight if the board lacks sufficient expertise for the practices to be effective.

In summary, agency theory suggests that boards have sufficient expertise to provide independent, substantive oversight of key firm risks. In contrast, institutional theory suggests that in the face of

uncertainty, boards will take actions that appear legitimate but may largely be only symbolic. To the extent that lack of domain expertise increases uncertainty, we expect nonexpert boards to adopt practices that appear legitimate but may lack effectiveness due to insufficient expertise. In such cases, boards will provide primarily ceremonial rather than substantive oversight.

3. Method

We used a qualitative field study approach because it is well suited for examining how processes and contexts influence how individuals behave and make decisions, especially for a contemporary phenomenon (Myers 2009, Yin 2018).[12] Thus, qualitative methods are required to open the "black box" of boards' governance of cybersecurity to understand how directors perform this fiduciary responsibility. In using this approach, we follow best practices for positivist, qualitative field study methods from recent accounting research to investigate our research questions (e.g., Malsch and Salterio 2016; Bills et al. 2018; Hayne and Vance 2019; Dodgson et al. 2020; Free, Trotman, and Trotman 2021).

To explore possible themes, theories, and issues relevant to cybersecurity oversight, we reviewed SEC and PCAOB reports and guidance on cybersecurity oversight, regulatory cybersecurity roundtables, and guidance from practitioners and academics (e.g., IIA 2010; SEC 2011; SEC 2018; PCAOB 2018; and NACD 2020). We also conducted preliminary interviews with professionals about the challenges that boards face in their cybersecurity oversight. This initial fieldwork helped us establish the theoretical lens for our study and to prepare an initial interview script (Yin 2018).[13]

3.1.Sampling Strategy

Because the focus of this study is on boards' oversight of cybersecurity, we conducted interviews with 20 directors of small-, medium-, and large-cap firms using a snowball sampling strategy. This yielded

[12] Approval for the use of human subjects in this research was granted by the institution in which the research took place.

[13] In developing our initial interview script, we solicited and incorporated feedback from multiple academics and professionals who specialize in cybersecurity.

an interviewee group that was diverse across a number of dimensions, as summarized in Table 1.[14] Panel A shows that among the 20 directors, 5 had cybersecurity expertise, which we categorize based on participants' self-assessments and our review of whether their work experience includes direct responsibility in cybersecurity management. All but three of the board members we interviewed had specific responsibility for cybersecurity as part of their membership of the audit committee or another committee tasked with overseeing cybersecurity in at least one of their companies. The other three directors participated in cybersecurity oversight as part of their broader board responsibilities.[15] The mean (median) number of director positions held by our director-participants was 2.75 (2.5).

Furthermore, because our research question investigates the nature of oversight provided, we also interviewed cybersecurity experts—executives (11 participants) and senior-level consultants (7 participants)—who support boards of directors. This allowed us to corroborate the perspectives of expert directors with those of individuals with bona fide cybersecurity expertise. The triangulation of different interview participants relative to a given corporate phenomenon is an important feature of many qualitative studies (Hayne and Vance 2019; Ody-Brasier and Vermeulen 2020; Brühne and Schanz 2022; (Miles et al. 2020). It is especially useful to substantiate observations from corporate "elites" (such as directors) with non-elites in organizational settings to avoid "provid[ing] only the 'top' part of a top-down perspective" (Odendahl and Shaw 2002, 314)."[16] For three of our director participants, we were also able to interview a CISO who reports to them. In these cases, we were able to directly compare the perspective of both parties in the oversight dyad.

[14] Two director participants and four executive participants represent private firms; in addition, some directors held both public and private positions. Surprisingly, we did not find any significant variation in the cybersecurity governance process between publicly held firms and privately held firms. When we asked the participants who had experience with both public and private boards about the differences between both (D-4, D-5, E-5), they indicated that cybersecurity oversight is similar. One director with multiple board positions said that their private firm had the best cybersecurity posture (D-15).

[15] We also interviewed board members without specific responsibility for cybersecurity because the SEC specifies that the board as a whole is responsible for cybersecurity (SEC 2018).

[16] Cohen et al. (2010) interviewed auditors to obtain an outside perspective on boards' oversight of financial reporting, while Beasley et al. (2009) interviewed board members. Noting this difference in perspectives, Cohen et al. (2010) suggested that there is a need for further research to probe whether auditors and board members have different experiences. In the spirit of this call, our interview pool allows us to compare perspectives of multiple parties involved in the cybersecurity risk oversight process.

Panel B of Table 1 presents information regarding the executive participants. While the participants' executive titles varied, all participants had direct responsibility for cybersecurity and reported to the board. As with our director participants, executives' firms represent both high- and low-technology industries. Panel C of Table 1 provides information on our consultant interviewees. We interviewed senior-level consultants across a range of firms that provide cybersecurity consulting services to boards, including large technology solution firms, the Big-4, and specialized consulting firms. In total, we conducted 41 interviews with 38 individuals.[17] We continued our snowball sampling process until the point at which novel insights were no longer obtained (i.e., we reached theoretical saturation; see, e.g., Morse 1995; Malsch and Salterio 2016)—both for our director participants and for our cybersecurity experts.[18]

3.2.Interviews

At least two researchers participated in each of the 41 interviews, which were conducted by phone or video calls and lasted an average of 50 minutes. We audio recorded and professionally transcribed all but four of these interviews. A graduate research assistant then reviewed each transcript against the corresponding audio recording to ensure accuracy. For the four interviews in which participants preferred not to be recorded, a researcher or a graduate research assistant took careful notes while two researchers conducted the interviews. Prior to each interview, we reviewed the participant's biographical information available from LinkedIn and any online biographies. For interviews with directors and cybersecurity executives, we also reviewed news articles, proxy statements, and annual reports relating to firms associated with the interviewees.

Before beginning each interview, we informed the interviewee that our objective was to understand how boards approach cybersecurity oversight. To encourage open and forthright responses, we also emphasized to them that their identities would be kept strictly confidential. At the start of the interview, we

[17] Three participants were interviewed twice to further explore themes they raised in the initial interview.

[18] Our coding process (described below) overlapped with our sampling process (i.e., we coded interviews while continuing to recruit participants), which helped us identify theoretical saturation. For example, during coding, each researcher independently identified themes raised in the interview. We then compared and evaluated whether additional interviews produced new themes or insights.

asked interviewees about their professional background to verify information we had collected about them and their company and to clarify their roles on the boards, or, in the case of cybersecurity executives and consultants, how they interface with the boards (Dodgson et al. 2020). We followed a semi-structured approach, customizing each interview script to the interviewee's position and background (see sample interview questions in Appendix A). The interviewees spoke freely and at length, with the researchers only interjecting to ask for clarification or to ask follow-up questions to further explore new insights or emerging themes raised by the interviewees. After each interview, the researchers held a debriefing to discuss the fit with our theoretical lens, emerging themes, and the possible refinement of our script.

3.3.Data Analysis

We analyzed our data in NVivo using an iterative process of coding (Saldaña 2013, Miles et al. 2020). In the first cycle of coding, a code "start list" was generated from emerging themes from early interviews, and all three researchers independently generated new codes based on three interviews to further develop the preliminary coding scheme (Miles et al. 2020). We did this through initial coding, a generative coding technique used to identify and label concepts that form the central ideas around a topic (Saldaña 2013). This initial coding resulted in many codes, which were then narrowed down based on thematic overlap to form our initial codebook with definitions. These codes broadly included dimensions such as the cybersecurity governance process, directors' attitudes toward cybersecurity, directors' cybersecurity expertise and its role in oversight behaviors, interactions between directors and cybersecurity executives, and cybersecurity oversight norms.

Next, all three researchers independently coded each interview. In this phase of the analysis, we continued to generate and discuss potential new codes (initial coding), and the relationships among the codes were examined to identify themes. In doing so, we used "simultaneous coding," or multiple codes for a single statement in cases where the data suggested more than one theme, especially relationships between codes (Saldaña 2013). After each interview was coded, each researcher independently took a memo of the main theoretical takeaways from the interview and of the proposed new codes. We then

discussed the major themes and codes of that interview. In addition, we used pattern matching to compare our categories and themes to conditions and mechanisms related to our theoretical lens, which provided new insights (Malsch and Salterio 2016, Yin 2018). We also looked for anomalous data that failed to conform to the expected patterns and emerging categories and themes and updated our themes and explanations accordingly (Miles et al. 2020). Throughout the coding, we reviewed coding differences among researchers to refine the codebook definitions and to create pattern codes of emerging themes (i.e., second cycle coding; Miles et al. 2020).

4. Main Findings

4.1. Findings of Boards' Oversight of Cybersecurity

An overarching theme of our findings is that cybersecurity has emerged as one of the top enterprise risks directors face because of the potential for companies across all industries (including traditional brick-and-mortar firms) to be taken offline due to a cybersecurity incident. Similarly, both expert and nonexpert directors expressed concern and even anxiety about a company they oversee becoming the next breached firm (e.g., Equifax or Colonial Pipeline) in the news. Accordingly, directors stated that cybersecurity merits oversight by the entire board, not just by those directors assigned to committees responsible for cybersecurity. This stated emphasis on oversight responsibility is consistent with agency theory, which predicts that boards will carefully monitor firm risks. However, contrary to the assumption of agency theory that the board possesses sufficient expertise to provide substantive oversight, all expert and nonexpert director participants also acknowledged that boards generally lacked expertise in cybersecurity compared to other domains, and that this posed challenges for their ability to perform effective oversight; however, our interviewees frequently reported that boards generally do not seek expert directors (a theme we return to at the end of this section).

Another overarching theme that participants uniformly identified is that nascent norms and the evolving cyber landscape are unique challenges for providing substantive oversight over cybersecurity relative to other areas, particularly given boards' general lack of expertise. Participants emphasized that

best practices for the oversight of cybersecurity risk are still being developed, and boards are struggling to understand their newfound responsibilities. Institutional theory predicts that boards will respond to such uncertainty by looking to regulators, peers, and professional groups (i.e., coercive, mimetic, and normative isomorphic pressures, respectively) to identify oversight behaviors that are seen as "legitimate." In our data, we find ample examples of all three categories of isomorphic pressures, and these pressures shape the way boards oversee cybersecurity.

Furthermore, a third overarching theme in our data is that uncertainty is greater when boards lack cybersecurity expertise. As an illustration of how isomorphic pressures can shape oversight behaviors, a nonexpert director described looking to professional groups such as the NACD and feeling an insatiable need for guidance on best practice: "[I get guidance from] wherever I can…[the NACD has] a tremendous education program, lots of great meetings all over the country. …but candidly, *I'll take that and more*." (D-17 nonexpert, emphasis added). An important issue is whether nonexpert board members can effectively oversee cybersecurity by adopting such best practices, or whether these behaviors are more likely to be symbolic. In the following subsections, we describe our field study findings on how expertise influences the degree to which boards provide substantive or superficial oversight, particularly in the areas of the board's engagement with cybersecurity oversight, questioning, relationship with management, and ability to detect false or withheld information on the part of cybersecurity management.

4.2.Board Engagement with Cybersecurity Risk

The boards of directors in our sample received the CISO's report annually, quarterly, or in some cases bimonthly—a clear indication of boards' attention to cybersecurity. Although at the time of our interviews most boards were not required by law to receive reports on cybersecurity from management, we found that regular reporting by the CISO was nonetheless a best practice. This is unusual compared to other areas of oversight because the CISO is often positioned one or more layers down from top executives in the organization, and therefore reports from the CISO to the board bypass the managerial chain of command. Other indications of board attentiveness reported by all our participant groups include receiving reports

from third-party security consultants, receiving board-tailored cybersecurity training from the CISO or organizations such as NACD, and asking questions about cybersecurity. Citing these efforts, both expert and nonexpert board members expressed that they exercise diligence when it comes to cybersecurity oversight:

> *I think we work really hard at this, and I think most boards do. …most of the failures are not failures of inattention. I think they're failures of you can't do everything in one day, and there's a thousand people trying to break into the system. … I think we've been very diligent, and we spend a lot of time and energy and knowledge on this, and we access whatever resources we need to do a good job. So, I feel pretty good about it.* (D-2 nonexpert)

Despite directors' efforts to adopt these recent security best practices, interviewees in all our participant groups shared that boards' engagement with cybersecurity is moderated by directors' level of expertise. Even nonexpert directors acknowledge that directors with low expertise are more likely to sideline themselves. Some director participants indicated that they are brought onto boards for their particular expertise and are more likely to jump in when a discussion is in their domain. Similarly, low cybersecurity understanding may make a director less likely to ask questions because "if you don't know, you don't want to ask questions" (E-5). oversight of cybersecurity is largely motivated by and limited to compliance concerns, although the board receives a report from cybersecurity management, directors may only passively listen in.

Although past research suggests that directors with low expertise engage less in oversight of the related domain (Beasley et al. 2009, Couchoux 2023), the domain of cybersecurity oversight is noteworthy in at least two ways. First, for many nonexpert directors, oversight of cybersecurity is largely motivated by and limited to compliance concerns and/or implementing best practices, sometimes at the expense of seeking to understand and address a firm's specific cybersecurity risks. Thus, some boards may perform cybersecurity oversight symbolically because the practices they adopt are not tailored for their firm or are not implemented effectively. Although nonexpert board members recognize that cybersecurity is an increasingly important enterprise risk, many focus on the performance of emerging best practices and norms to "keep pace" with their peers (D-7 nonexpert). For example, the board may feel that they have checked a

box with cybersecurity oversight because they received a positive report from the CISO in their last annual meeting. A consultant went even further: "[The board's] primary motive is compliance, or because their customers require them to do it. We're not at a point where there's this genuine, internally-driven incentive to do cybersecurity risk management well" (C-3). In contrast, directors with high security expertise focus on security concerns beyond mere compliance or adherence to best practices.

Another prominent characteristic of cybersecurity oversight is that, with nonexpert boards, attention is often reactive, piqued by cybersecurity incidents. Many CISOs described receiving more questions about cybersecurity after prominent reports of breaches in the business press. Such external cyber incidents serve as a "wake-up call" in which board members are prompted to ask, "Could that have happened to us?" (D-5 expert, in reference to nonexpert directors). The problem with this approach is that "If [a director is] just focused on today's needs—if you live in the news—you're not doing a good job" (E-6). An expert director described how nonexpert directors' interest in cybersecurity can quickly change from a compliance mindset following an incident: "They think of their briefing as compliance and an exercise until they get hacked. And then, of course, they're very interested in the details" (D-12 expert). However, this type of engagement wanes as a security incident becomes less salient in nonexpert directors' minds. In contrast, for directors with high expertise, engagement with cybersecurity remains relatively constant.

A powerful example of how directors' expertise determines whether their engagement with cybersecurity is substantive is when directors voluntarily make efforts beyond formal oversight processes, which we term "stepping up." This type of oversight is described as unstructured, self-selected, and undertaken by directors who either desire to learn more about security or have expertise in cybersecurity. Stepping up can take a variety of forms, such as meeting regularly with the CISO, acting as an intermediary between the CISO and the board or CEO, and advocating for increased cybersecurity budget allocations, among other actions. These "stepping up" actions are more likely to take place when a director has expertise because low-expertise directors typically lack the interest or capacity to understand details of a security program. Digging into the details of a security program can entail a substantial time investment even for an expert director, and much more so for a nonexpert.

When an expert director steps up, they are able to provide critical feedback on cybersecurity programs. For example, one expert director initiated a "deep dive" into the firm's cybersecurity program to learn about the firm's cybersecurity systems and issues:

> *As a sitting CIO and someone who has grown up in the cyber space, I certainly wanted to see a little more focus on [cybersecurity] and a little more structure, which is why I suggested to the board that we have an independent review, and at first, their question was "Why, what are you worried about?" I said, "I don't know. I don't know what to be worried about if I don't know."* (D-5 expert)

This engagement from the director with cybersecurity expertise prompted substantial additional work from the CISO and the security team in making necessary improvements. The CISO at this organization admitted:

> *[Without D-5 stepping up], I don't know that we ever would've had this maturity model in place. … certainly, we wouldn't have done that third-party review… You're forcing me to face the reality that … [D-5] giving us that kick in the ass, frankly, was probably one of the better things that happened to us. It forced us to really start to look at how we measure maturity and to understand what it's going to take to move those maturity curves forward, and what initiatives we need to take to move those things forward.* (E-2)

In contrast, if a nonexpert director chooses to step up, their actions may be less likely to lead to substantive oversight. For example, one nonexpert director volunteered to meet with the CIO and CISO bimonthly to conduct a "deep dive" on a "myriad of [security] issues" (D-20 nonexpert). However, without expertise, this exercise is "pretty overwhelming" because "the more you know, the more there is to know" (D-20 nonexpert). Furthermore, from the perspective of that firm's CIO, these meetings amount to "three to four hours of training" for the director, rather than providing oversight or immediate value to the security program (E-11). Thus, stepping-up efforts from nonexpert directors can increase the burden on executives without improving the security program.

Overall, we find that the level and effectiveness of engagement, which is fundamental to the oversight expected by agency theory, hinges on the expertise of directors. As one expert director put it "[B]oard members want to be useful. They want to make the company successful and therefore, they are inclined to speak more about it and dwell on things where they feel like they can contribute" (D-9 expert). Therefore, directors with low cyber expertise will instead "lean into" things they know (D-7 nonexpert) and engage in

cybersecurity oversight activities that, although appearing legitimate as emphasized by institutional theory, effectively result in superficial oversight, as we further illuminate below.

4.3.Questioning

Our interviews revealed that questioning is a primary form of board oversight of cybersecurity, consistent with prior board literature in other domains (e.g. Gendron and Bédard 2006; Beasley et al 2009; Kang, Trotman and Trotman 2015). Nonexpert board members suggested that their general oversight experience enabled them to intuitively know the right questions to ask. As one director put it:

> *Most boards are filled with pretty smart people, and we're not afraid of not knowing what we don't know. We ask a lot of questions and require that we get answers….We ask the right questions, we get the right people in front of us. I think we make good, sound judgments and do our duty in spite of the fact that we don't have all this cyber background.* (D-3 nonexpert)

However, despite nonexpert directors expressing confidence in boards' ability to ask effective questions, interviewees in all our participant groups drew a contrast between board members' ability to ask questions about financial risk (an area cited by participants that nearly all directors were familiar with) versus cybersecurity risk. Furthermore, most expert director, executive, and consultant participants shared that nonexpert directors are more likely to ask fewer, basic, or perfunctory questions.[19] Table 2 presents a summary of the contrasting opinions on the effect of expertise on questioning by participant expertise.[20]

Several notable and novel phenomena in director questioning emerge from our interviews. First, a substantial portion of nonexpert questions in the cybersecurity oversight domain are educational in nature. Many expert director, executive, and consultant participants described nonexpert directors asking questions to improve their general understanding of cybersecurity and related risks (e.g., what are the risks and how incidents in the news relate to their firm) rather than questions that provide substantive oversight of the firm's cybersecurity program. These expert interviewees stated that directors without expertise are limited

[19] An example of a basic question is, "Hey, what are we doing for cybersecurity?" (E-2, D-11 expert in reference to nonexpert directors). Example of questions that reflect expertise in cybersecurity are, "Do we encrypt our source code? Do we actually carry PII in unencrypted form? Are we PCI compliant on our credit card transactions? Do we actually throttle the database such that you cannot pull all customer records at one time?" (D-11 expert).

[20] Tables 2–4 summarize participant responses, illustrating where consensus and deviant cases exist.

in their ability to ask effective questions because they "don't know what they don't know" (C-1, D-11 expert), and "don't know what they want to know" (E-3). Second, some expert interviewees described the tendency of nonexpert directors to depend on lists disseminated by professional groups (e.g., NACD) for questions directors "should" ask without fully grasping the question. Third, some of our participants shared that expertise affects whether a director is capable of holding a dialogue in response to questions. For example, a CISO's response can be so technical that nonexpert directors are unable to understand and assess its adequacy. Reflecting on this problem, an expert director observed that nonexpert board members may get "lost" during management's cybersecurity briefings:

> *Frankly, CISOs and the typical [director] speak two different languages. The CISO speaks a systems engineering or computer science language... And the people typically on the boards are lawyers or MBAs. And they speak an entirely different language. So, a CISO can brief a board, and they all nod and thank him or her. And there will have been no communication because one is speaking and the other one doesn't understand… it's kind of a dialogue of the deaf.* (D-12 expert)

Thus, although nonexpert directors may ask questions drawn from respected sources (i.e., questions that are perceived as legitimate), their lack of expertise makes the questioning superficial in terms of the oversight provided. In the words of one consultant, "That doesn't mean that they understand the answers, and that doesn't mean that they know what to do about it… [B]oards are getting smarter and smart enough to ask the questions—they're just not yet smart enough to interpret what the CISO is saying (C-7)"

In contrast, most interviewees shared that cybersecurity expertise allows directors to ask "better" (E-4), "good" (D-2 nonexpert, E-2, D-5 expert), "intelligent" (E-2, D-12 expert), "tough" (E-8), or "the right" (C-1, D-7 nonexpert, E-3, D-8 nonexpert, D-11 expert, C-6, E-8) questions. An expert director offered examples of probing questions, noting that, *"*You will not know to ask those questions if you haven't come from that domain and seen the kind of [expletive] that happens when people get hacked" (D-11 expert). The difference in question quality based on expertise levels was explained by a self-described "inexperienced" director who referred to a colleague with more expertise: "His questions just might be a little bit better because he knows where some of the stumps are underneath the water" (D-8 nonexpert). In addition, expertise can help a director exercise restraint, asking only questions that add value. Finally, just

as expertise enables directors to ask better questions, expertise similarly allows directors to understand the answers they receive from executives. Further, expert interviewees described expertise as particularly important for enabling a director to ask valuable follow-up questions. A consultant explained:

> *It's not the first question that you ask because you can download the dummy's guide to cybersecurity. It's the second, and third, and fourth, and fifth questions that go off of the branching logic, based on how the CISO is providing his or her updates.* (C-6)

The foregoing findings underscore the implicit assumption of agency theory that directors have sufficient expertise to provide substantive independent oversight (Fama and Jensen 1983, Jensen 1993). From the above examples, our participants perceive expertise to lead to higher question quality and dialogue and more substantive oversight, consistent with predictions from agency theory. Our evidence suggests that both expert and nonexpert directors seek to provide oversight of cybersecurity by asking questions of the CISO and other cyber executives. In this way, nonexpert directors exhibit legitimate questioning behaviors. However, because the effectiveness of questions depends on expertise, questioning from nonexpert directors ultimately lacks substance and effectiveness, and therefore primarily results in a symbolic oversight exercise, aligning with predictions from institutional theory.

4.4.Relationship with Cybersecurity Management

Both expert and nonexpert directors we spoke with generally emphasized the importance of working together with management to figure out the best way to manage cybersecurity risk, and frequently described being on the "same team" as cybersecurity executives. That boards focus on their collaboration with executives rather than their role in mitigating agency costs is not unique to the cybersecurity setting (Edmans et al. 2023). However, we found that nonexpert directors are willing to rely on CISOs to an unusual degree due to their lack of familiarity with this growing and evolving subject matter. Cybersecurity executives and consultants described this sort of support of the board as "coaching," (D-9 expert executive director, C-5, C-6) a term that we use to label a range of activities in which boards highly rely on the CISO. Participant-provided coaching behaviors include educating the board about cybersecurity, conditioning

them to the type of information they should receive in reports, and guiding their decisions. One executive described this heavy reliance as follows:

> *[Y]ou typically don't have to explain to members of the audit committee how a financial statement works. That's just implied and understood that they are masters of that and have a tremendous depth of experience in how to look at that and ask the right questions related to it. [I]n comparison, [cybersecurity is] a topic that everybody's trying to really figure out, "What does it mean?"* (E-1)

For example, our participants indicated that when board members lack adequate cybersecurity experience, educating the board is an important part of the CISO's responsibilities. This involves talking with individual board members to determine their level of understanding of cybersecurity, and then personally providing "Security 101" training to "level set," get "on the same page," and provide "a common language" relative to cybersecurity for all directors (E-3, E-6, D-7 nonexpert, E-9, D-14 nonexpert, C-7, D-16 nonexpert). CISOs described efforts to "raise the cyber-IQ" (E-4) of the board over time by offering training as part of regular board meetings, and meeting informally with board members to answer their questions about cybersecurity concepts and current events. When asked to describe such training from cybersecurity management, one nonexpert director said: "it was really eye-opening, and scary actually, of where the biggest threats are, what some of the tactics are, …how some of these things are evolving" (D-16 nonexpert). One consultant pointed out that even budgetary requests may require the CISO to instruct the board, "Everybody knows what fire extinguishers are, so you don't have to tell people what they're for," but when CISOs request funding to purchase cybersecurity software or services, they must explain what they are, what threats they mitigate, and the potential consequences of not acquiring them (C-1).

Beyond receiving training from CISOs, nonexpert directors also require CISOs to set expectations for how a security program should function and the levels of risk that are appropriate. For example, one CISO presented a widely used cybersecurity framework to the board and explained, "This is what a good program should look like" (E-3). Other examples include a CISO explaining to the board what level of a cybersecurity maturity model would be appropriate for the firm to target (a highly strategic decision), and a CISO negotiating with the board about realistic expectations of the inevitability of data breaches.

Nonexpert directors also often do not know what information about the cybersecurity program they should review to provide oversight. In such cases, CISOs not only set expectations, but also determine what is reported to the board. One CISO explained, "[T]he boards really don't know what they want to know… And so, we're all going through this process of developing 'what should the board see?' and 'what should they care about?'" (E-3). Another CISO described steering the board to a particular form of cybersecurity audit because "they didn't know what they were asking for" (E-5). In a particularly circular example of governance, some CISOs provide boards with lists of questions to ask.

In contrast to the relationship that nonexpert directors have with CISOs, expert directors do not require education from management, as they already have understanding and awareness of cybersecurity threats. Similarly, directors with high expertise do not require that expectations be set for them because they already "know what good looks like" (D-5 expert, C-6), and they know what information they want reported to them. Thus, rather than needing "coaching" from management, expert directors can independently evaluate management's cybersecurity efforts and "challenge" (D-12 expert, E-8) management on issues that arise. An executive observed:

> *[Having a cybersecurity expert on board] really calls and exacts more of the CISO who is going into the [meeting with the board], knowing that there's that kind of expertise on the board and what you might be asked about and what you need to be prepared to answer.* (E-7)

More broadly, expert board members can assess the quality and/or fit of the CISO for the organization and direct management to replace the CISO when needed. This is less likely to occur when nonexpert directors are dependent on the CISO for coaching.

Although boards receiving reports directly from the CISO is a best practice and is required by regulation in some industries (e.g., the updated 2023 FTC Safeguards Rule for financial institutions), the analysis above illustrates that it is unlikely to result in substantial oversight if directors lack sufficient cybersecurity expertise. In such cases, their uncertainty surrounding the oversight of cybersecurity leads to boards effectively ceding key aspects of their oversight role to the CISO. This expertise gap gives rise to circular governance, whereby the subjects of oversight (in this case, CISOs) are able to significantly

influence the nature and terms of the oversight by setting benchmarks for adequate security programs, what cybersecurity oversight should entail and how it should be conducted. Overall, this dynamic is not consistent with the expectations of agency theory that boards provide independent oversight. Instead, in line with institutional theory, our findings suggest that boards with low expertise perform legitimate actions (i.e., receiving reports from CISOs) that ultimately result in symbolic oversight.

4.5.Detecting False or Withheld Information in Management Reports

A particularly stark manifestation of the agency conflict between the board and the CISO is the tendency of the latter to filter cybersecurity reports to improve the board's assessment of the CISO's performance. Clearly, management obfuscating information is not isolated to the cybersecurity setting, as extensive studies have examined information asymmetry between the board and better-informed managers (Adams and Ferreira 2007, Duchin et al. 2010, Schwartz-Ziv and Weisbach 2013, Free et al. 2021). However, our interviews suggest that this asymmetry (and, hence, the potential for obfuscation) is especially high in the cybersecurity setting due to a general lack of cybersecurity expertise among directors.

Due to the sensitive nature of this issue, we asked participants whether it was common for CISOs in other companies to filter their reports. We find that most nonexpert directors believe that CISOs are unlikely or unable to obfuscate. For example, one such director commented, "I think most of the CISOs I have seen are like internal auditors. They're not trying to hide things" (D-10 nonexpert). In contrast to this view, among the executives and consultants we interviewed, the majority held the belief that some CISOs obfuscate their reports to boards to make themselves or other executives look better. For instance, a CISO candidly shared his/her experience under a prior CIO (who was above the CISO in the organizational hierarchy):

> *[The former CIO] always used his presentation [to the board] to sell.… That is my perception of how it was. Paint your performance in the best possible light—that was my direction at all times. "Yeah, we're perfect, we're on track with our plan." In reality, it wasn't as smooth as we presented to the board.* (E-5)

To corroborate our expert interviewees' views that opportunistically filtering reports is a common practice, we surveyed an additional 33 CISOs.[21] In response to the question, "From your impression of firms in general, what percentage of CISOs filter their reports to the board to make themselves or their superiors look better?", the mean (median) is 42% (40%) of CISOs, and all but one respondent reported a nonzero percentage.[22]

Similarly, expert directors were more aligned with our CISO and consultant participants on this issue, as all but one acknowledged the potential for CISO obfuscation (see Table 3). On this issue, an expert director said, "I think there's always that risk and I think that a board should have a high awareness and concern for that" (D-5 expert). Another expert director, when asked whether CISOs might be able to successfully filter or provide false information to the board because most board members have low cybersecurity, replied, "Of course. All the time," (D-12 expert). This individual elaborated further:

> *If you were to look at any of the board briefings that I've seen, they are not helpful. They're either intended to be at such a high level of abstraction that the board can't get into their knickers. Or alternatively, they are so geeked up that the board can't understand it. Now, is that intentional? I don't know, you'd have to get into motives. But it certainly has the effect that the briefing occurs, there are one to two perfunctory questions, then they move on.* (D-12 expert)

Thus, we conclude that CISOs opportunistically filtering reports to boards potentially limits the effectiveness of board oversight, although nonexpert directors downplay this concern.

In addition to this difference in perception regarding CISO filtering, cybersecurity expertise also enables directors to know "the right questions to ask, such that they can decipher truth from fiction or snow from reality" (C-6) and to "smell out a situation where management may be whitewashing a particular subject" (E-3). Expert directors can push back against CISOs who skirt around the root issues or report diversionary information. One expert director explained that with expertise, directors "want to see real

[21] We administered the survey to members of Gartner's CISO Coalition, a large network for collaboration and information sharing that has CISOs and other cybersecurity executives among its members. Two invitations to take the survey were sent via email, yielding a response rate of 2%.

[22] In white-collar crime studies in criminology, it is assumed that respondents self-censor their reports of socially undesirable behavior. Therefore, any nonzero response is considered meaningful (Paternoster and Simpson 1996, Piquero et al. 2016). In addition, asking about behavior of respondents' peers is a common way of reducing social desirability bias (Fisher 1993).

metrics. They will go into a deeper level of detail. And the most important thing is that they understand what the CISO is saying. And they can challenge her" (D-12 expert).

Consistent with our previous findings for other oversight activities, expertise affects directors' perceptions of the risk of CISO filtering, as well as directors' ability to detect such filtering. Our finding that many directors downplay incentive conflicts is inconsistent with expectations from agency theory. Rather, nonexpert directors ceremonially receiving reports (a legitimate practice) without recognizing managers' incentives or ability to obfuscate information is more consistent with institutional theory.

4.6.Why Do Boards Not Seek to Acquire Cybersecurity Expertise?

Our director participants unanimously cited cybersecurity as one of the most critical enterprise risks that the board must oversee. However, our findings in the previous section indicate that when boards have insufficient expertise in this area, they respond to their responsibility for cybersecurity oversight by taking actions that follow best practices that are legitimate in form (e.g., receiving reports from CISOs and asking questions) but ultimately lack substantive effect. As discussed previously, agency theory presumes that boards will have sufficient expertise to provide effective oversight. Based on the survey evidence cited in Sections 1 and 2, cybersecurity expertise is generally lacking in boards. We corroborated this survey evidence by analyzing proxy statements for a random sample of 1,000 firms from the Russell 3000 Index. Specifically, we examined the prevalence of cybersecurity among directors' disclosed skills and qualifications, which firms are required to describe under Regulation S-K. We find that only 14.7% of firms disclosed at least one director with cybersecurity or related skills and experience, consistent with another contemporary analysis (Rundle 2023).[23] Thus, we observe in archival data that appointing directors with cybersecurity expertise does not appear to be a priority for most boards, and our interview data suggest that this as a continuing trend. A natural question then arises: If directors believe cybersecurity is a critical enterprise risk for boards to oversee, why do boards not seek to acquire cybersecurity expertise to enable them to provide substantive oversight as predicted by agency theory?

[23] Furthermore, only 13.2 percent of the firms specifically referenced experience related to cybersecurity or privacy in the biographies of their board members.

Our participants provided several reasonable explanations for why boards do not appoint cybersecurity experts to the board. These explanations can be divided into two main types. First, participants describe practical constraints faced by boards when appointing directors with cybersecurity expertise. For example, participants shared challenges in such hiring due to the scarcity of bona fide cybersecurity skills in the director labor market. A related reason is the common perception that directors with cybersecurity expertise will have little to contribute to the board beyond cybersecurity, and that companies should not "waste [a] board seat" on a one-trick-pony cybersecurity expert who cannot contribute to other areas of the business (D-5 expert) and that third-party experts can be engaged to fill the gap (D-4, nonexpert). Others felt that the mere presence of a director with cybersecurity expertise on the board could cause the rest of the board to over-rely on that person or create a false sense of security. Others point to the recency of cybersecurity's emergence as critical enterprise risk as a reason why there is a lack of expert directors in this area.

Although apparently genuine, these sentiments do not seem to satisfactorily explain the expertise gap. Boards of large companies could likely attract directors with cyber expertise if they wanted to do so, notwithstanding the shallow talent pool of cyber experts.[24] Likewise, board size is not necessarily constrained and could accommodate additional directors with cybersecurity expertise if such skills were perceived as necessary. Finally, because the SEC has agitated for corporate cybersecurity disclosures since 2011 (with additional emphasis added over time; SEC 2011, 2018, 2023), insufficient time does not seem to be an adequate explanation on its own.

A second and more compelling reason for why boards do not prioritize appointing cybersecurity experts that was found in our analysis is that many nonexpert directors believe they are able to provide adequate oversight of cybersecurity by virtue of their general experience, notwithstanding their lack of specific expertise. For example, nonexpert directors expressed that their general business experience and abilities as board members adequately qualified them to oversee cybersecurity risk. This may stem in part

[24] To illustrate, one of our participant-boards is a Fortune 100 company that lacks a cybersecurity expert despite its industry being sensitive to cybersecurity threats and the board experiencing recent refreshment.

from a failure to recognize potential agency conflicts between themselves and the CISO, such as the latter's incentives to filter reports to the former. A similar sentiment shared by nonexpert directors is that broad business experience is more valuable than deep expertise in cybersecurity because broad experience allows directors to have "big-picture judgment" and that "we're in the judgment business, we're not in the expertise business" (D-4 nonexpert). One director's comment represents the nuanced way many participants view bringing on a cybersecurity expert:

> *I see this debate a lot about 'do we need a cyber expert?', and my personal opinion on that is many of us have dealt with cyber in managing our own companies, …, but to get someone who was a former CISO, they may not make the best board member because they don't have the broader experience. I think we should be relying on the company hiring great expertise to manage the risk and us being at more of the oversight role. Having said that, [Cybersecurity] is so high on the list of risks because just the nature of the subject matter is one that, even if you were an expert five years ago, you might not be so expert today. It's a tough area to manage.* (D-16 nonexpert)

One nonexpert director went so far as to argue that a lack of technical expertise can be a strength if a director has a holistic understanding of business risk:

> *[S]ometimes, people with the least technical knowledge in many ways have a better perspective on understanding business risk and enterprise risk associated with it, but they're thinking about it in [a] holistic context [rather] than dropping you down into this technical silo.* (D-6 nonexpert)

These statements can be viewed as assertions of directors' own legitimacy, and their ability to provide oversight by virtue of their general experience as directors. As discussed above, nonexpert directors pointed to their boards' following emerging best practices, such as their asking "the right questions" (D-3 nonexpert), receiving reports and other regular interactions with CISOs, as evidence of the legitimacy of their oversight. In addition, nonexpert directors pointed to cybersecurity training through NACD or similar professional organizations as aiding their oversight role. Non-expert directors' executive experience at a digital or technology firm was commonly cited as a source of adjacent expertise that enables boards to provide adequate cybersecurity oversight. Finally, several nonexpert directors cited their ability to contract consultants to compensate for their boards' lack of cybersecurity expertise.

In contrast, our expert participants provided a strong counterpoint to the above arguments and saw directors' lack of expertise as a major impediment to effective oversight (see Table 4 for a summary of

these contrasting opinions by participant expertise). For example, addressing the argument that general expertise qualifies boards to oversee cybersecurity, an expert director offered a stark refutation:

> *[M]ost boards are simply completely incapable of overseeing cyber risk. It's just so far outside of their experience and their expertise that all they can do is assess the credibility of the executives that are put in front of them.* (D-9 expert)

Expert participants were skeptical that brief training sessions could provide the expertise needed to provide substantive cybersecurity oversight. Furthermore, experts were careful to point out that technology expertise is not the same as cybersecurity expertise because "cyber is its own discipline" with "a different mindset and a different set of tools" (D-9 expert).[25] Expert participants argued that relying on consultants for cybersecurity expertise can effectively result in outsourcing oversight and that nonexpert directors may not be able to determine what type of cybersecurity engagements are needed, nor be able to evaluate the quality of consultants' work. Finally, expert participants pointed to the hollowness of following best practices without expertise because of a failure to understand and to "know what good looks like" (D-5 expert).

An interview with a nonexpert director who invited the company's CISO to join the interview provided a striking illustration of the gap between experts and nonexperts regarding the perceived importance of board-level expertise. When asked whether having a board-level expert would make a difference in the oversight of cybersecurity, the director blithely responded, "I don't see how it would" (D-18 nonexpert); however, the executive candidly shared a contrasting belief, claiming that an expert director on the board would result in more structured and in-depth oversight.

In summary, our field study demonstrates contrasting opinions about the need for cybersecurity experts on boards. Experts generally believe that substantive and independent assessment is not possible without domain knowledge that comes from actual work experience. While acknowledging that cybersecurity expertise is helpful, the majority of nonexpert directors shared that they do not believe

[25] It is well known in the IT space that cybersecurity is its own domain that is often in conflict with IT project development, so IT expertise studies may not translate to cybersecurity risk oversight.

effective oversight requires domain expertise. They provide practical reasons for not appointing experts, but more revealingly, they assert that their current oversight based on general business expertise supplemented with third-party consulting is sufficient for effective oversight.

5. Discussion and Conclusion

Our participants uniformly perceive cybersecurity risk oversight to be a key and emergent board responsibility in a domain rife with uncertainty, which is exacerbated for nonexpert directors. Consistent with institutional theory, we find that directors respond to this uncertainty by seeking legitimate practices reflecting isomorphism. We further find that domain experts believe that even well-intended performance of isomorphic best practices results in essentially ceremonial oversight in the absence of genuine expertise. Moreover, nonexpert directors are less likely to see a meaningful difference in effectiveness between expert and nonexpert directors because they believe that their performance of best practices provides legitimate oversight, and therefore do not see the need to appoint directors with bona fide cybersecurity experience. In contrast, expert directors, executives, and consultants we interviewed see a clear difference in oversight performed by experts versus nonexperts and argue for the need for cybersecurity experts to be placed on boards to provide an independent check on cybersecurity management.

Overall, we find that neither agency theory nor institutional theory uniformly explains boards' cybersecurity oversight. Instead, our analysis shows that bona fide cybersecurity expertise is a key contingency that determines whether substantive or symbolic oversight is performed, as predicted by agency theory and institutional theory, respectively. In other words, expertise is a boundary condition for whether agency theory or institutional theory better explains boards' oversight of cybersecurity. This study therefore contributes an important theoretical contextualization of agency theory and institutional theory in the domain of cybersecurity oversight (Johns 2006, 2017).

Our study provides a number of novel theoretical insights compared to prior research. First, Gendron and Bédard (2006) interviewed various audit committee meeting participants in three large Canadian firms and find that audit committee members reflectively believe they are effective because they have domain

(i.e., financial) expertise. In contrast, in our study, we find that directors believe they are effective *even without* domain expertise due to their general board experience. Second, Gendron and Bédard (2006) find that ceremonial features of governance, such as regular meetings with management, provide a sheen of effectiveness, even in the eyes of managers and auditors who support the audit committee. In contrast, the executives and consultants we interviewed generally did not perceive such ceremonial features as effective when expertise was lacking.

Third, several recent studies find that management can have an outsized influence on the terms of board oversight (e.g., Cohen et al. 2002; Beasley et al. 2009; Cohen et al. 2010; Clune et al. 2014)[26], similar to the circular governance we document. These papers often point to CEO power and board–CEO social ties as being key factors leading directors to cede oversight control to management. In our setting, however, nonexpert directors over-rely on management and allow the supposed subjects of oversight to dictate how oversight is conducted due to a gap in expertise rather than power. Unlike CEOs, the CISOs in our study are not considered "powerful," as they often struggle to achieve legitimacy within the executive suite (Lowry et al. 2022). Thus, we contribute a novel explanation for why boards cede control to management even in the absence of power imbalances or social connections.

Fourth, prior research interprets ineffective oversight as the result of boards adopting ritualistic practices that appear legitimate to *external parties*. In contrast, in our setting, we find that nonexpert board members respond to the uncertainty inherent in cybersecurity risk oversight by seeking out and performing best practices they *themselves* believe are legitimate, notwithstanding the fact that experts view these efforts as ineffective. An implication of our findings is that increasing directors' motivation is unlikely to lead to improved effectiveness in the absence of bona fide expertise. For example, Cohen et al. (2010) proposed that "fear of legal liability" (p. 783) may drive a shift from symbolic to substantive board oversight. Because our nonexpert director participants already perceive that following legitimate best practices results in effective oversight, increasing board incentives is likely to have little impact on cybersecurity outcomes.

[26]Relatedly, Fiolleau et al. (2019) find that audit committees sometimes over rely on auditors to raise concerns about the audit.

We find that in cases when nobody on the board has bona fide expertise, directors resort to oversight behaviors they view as substantive and adequate, but which, lacking expertise, are effectively symbolic gestures only. This suggests a potential blind spot in directors' self- and board-level evaluations.

We answer calls for additional research to examine the role of audit committees (Beasley et al. 2009), especially relative to emerging oversight responsibilities (Hermanson et al. 2023). Importantly, our setting is characterized by scarcity in domain expertise, which contrasts starkly with recent qualitative studies touching on the role of financial expertise on the audit committee. For example, all three audit committees in Gendron and Bedard's (2006) study are characterized as having an "extensive financial and accounting background" (p. 219). Similarly, Couchoux (2023) notes that financial literacy is a baseline requirement for audit committee members of public companies and finds that audit committee members' conceptualization of their knowledge informs their financial reporting oversight styles. Importantly, Couchoux's (2023) financial reporting setting gives space for directors to choose complementary oversight styles that align with the relative financial expertise among audit committee members. We extend Couchoux's findings by investigating a setting wherein complementary oversight styles are not available due to low overall expertise. We do this by triangulating the perspectives of expert and non-expert directors with those from consultants and cybersecurity executives. Our unique setting allows us to provide rich examples of how directors' domain expertise influences oversight behaviors. Along these lines, we contribute a novel account of how boards conduct cybersecurity oversight. Our findings suggest that cybersecurity risk and its oversight are inherently uncertain, and that directors with lower expertise perceive greater uncertainty with regards to this risk and its oversight, which then encourages oversight isomorphism, as predicted by institutional theory.

Our results have implications for the ongoing debate about the necessity of cybersecurity expertise at the board level and whether or how it should be required for public firms (Larcker et al. 2017, SEC 2022). While our participants unanimously perceived board-level cybersecurity expertise as being helpful, our interviews revealed that experts and nonexperts often have opposing views on whether cybersecurity

expertise is a requirement for effective oversight.[27] Our analysis suggests an increased potential for cybersecurity-related corporate governance failures when nonexpert boards cede control of oversight. However, we are careful to note that the policy implications of our findings are not obvious. For example, our study does not encompass a full examination of the relative benefits of cybersecurity expertise versus other director qualifications. Thus, while we do not attempt to directly investigate the costs and benefits of requiring cybersecurity expertise at the board level, we believe that our study provides useful insights for policymakers and shareholders as they make decisions relative to board qualifications.

This study is subject to similar limitations as other interview-based field studies. For example, our participants may not have been fully candid in their responses. We attempted to mitigate this concern by interviewing directors with and without expertise as well as CISOs and consultants who advise boards. However, it is possible (and perhaps even likely) that our interviewees' responses reflect self-serving biases about the role of expertise. For instance, we find that directors with expertise emphasize its importance, while directors without expertise downplay its significance. Nevertheless, our interviews yielded a range of perceptions, many based on participants' experiences with multiple boards with varying levels of cybersecurity expertise. A second limitation is that because our interviews were semi-structured and were subject to participants' time constraints, not all interviewees were asked every question. Given the nature of our methodology, we are unable to generalize our participants' experiences in the statistical sense. However, our participants often shared experiences from multiple firms with which they had been involved (particularly our board and consultant participants), and our analysis of later interviews exhibited theoretical saturation. For these reasons, we believe the perceptions we describe generalize beyond the firms in our study (Lee and Baskerville 2003).

[27] Perullo (2021) explains that CISOs in different organizations may take a primarily expert opinion/oversight role, as distinct from a resource provision and risk management role. In organizations where the CISO is viewed as providing oversight, the board may not perceive a conflict in relying on the CISO (more similar to how they would rely on the internal auditors). Although this situation did not arise in our data, we acknowledge this possibility and that in such cases the debate for the need for board expertise of cybersecurity may be more nuanced.

Our study suggests several avenues for future research. We focus specifically on cybersecurity risk oversight, and while we propose that our findings are relevant to other domains, especially emerging board responsibilities characterized by high uncertainty, further research can examine the generalizability of our findings to other board oversight areas, such as DE&I and ESG. In addition, prior research has found both positive and negative effects of board background diversity (e.g. Anderson, Reeb, Upadhyay and Zhao 2011; Adams, Akyol and Verwijmeren 2018). It may be that the costs of director skill diversity found by Adams et al. (2018) was partially caused by directors' perceptions that anomalous directors are "one-trick ponies" that cannot contribute in other areas, consistent with the reservations expressed by the nonexpert directors we interviewed. Also, prior studies show that nominating committees emphasize chemistry between directors (Clune et al. 2014), which may reflect the fact that director appointments are also subject to isomorphic pressures toward director homogeneity (Cohen et al. 2008b). Our study provides evidence for the benefits of uncommon director skills and for resistance to non-traditional director backgrounds. Future research can explore the extent to which the lack of directors with cybersecurity (and other nontraditional) expertise is driven by the tendency of boards to attract directors with homogenous backgrounds, as predicted by institutional theory (Tuttle and Dillard 2007).

References

Abbott LJ, Parker S, Peters GF (2004) Audit committee characteristics and restatements. *Auditing: A Journal of Practice & Theory* 23(1):69-87 Article.

Adams RB, Ferreira D (2007) A theory of friendly boards. *The Journal of Finance* 62(1):217-250.

Adams RB, Akyol AC, Verwijmeren P (2018) Director skill sets. *Journal of Financial Economics* 130(3):641-662.

Agrawal A, Chadha S (2005) Corporate governance and accounting scandals. *The Journal of Law and Economics* 48(2):371-406.

Aguilar LA. (2014) Boards of directors, corporate governance and cyber-risks: Sharpening the focus. *Cyber Risks and the Boardroom*. New York Stock Exchange, New York, NY, Accessed July 22, 2020, 2020, https://www.sec.gov/news/speech/2014-spch061014laa#_edn26.

Anderson R, Reeb D, Upadhyay A, Zhao W (2011) The economics of director heterogeneity. *Financial Management* 40(1):5-38.

Ashraf M, Michas PN, Russomanno D (2020) The impact of audit committee information technology expertise on the reliability and timeliness of financial reporting. *Accounting Review* 95(5):23-56 Article.

Baugh M, Hallman NJ, Kachelmeier SJ (2021) A matter of appearances: How does auditing expertise benefit audit committees when selecting auditors? *Contemporary Accounting Research* (forthcoming).

Beasley MS (1996) An empirical analysis of the relation between the board of director composition and financial statement fraud. *Accounting Review* 71(4):443-465.

Beasley MS, Carcello JV, Hermanson DR, Neal TL (2009) The audit committee oversight process. *Contemporary Accounting Research* 26(1):65-122.

Bédard J, Chtourou SM, Courteau L (2004) The effect of audit committee expertise, independence, and activity on aggressive earnings management. *Auditing: A Journal of Practice & Theory* 23(2):13-35 Article.

Bills KL, Hayne C, Stein SE (2018) A field study on small accounting firm membership in associations and networks: Implications for audit quality. *The Accounting Review* 93(5):73-96 Article.

Bloomfield R, Nelson MW, Soltes E (2016) Gathering data for archival, field, survey, and experimental accounting research. *Journal of Accounting Research* 54(2):341-395.

Blosfield E (2021) Maine one of latest states to enact NAIC-inspired Insurance Data Security Act. *Insurance Journal*, May 6, 2021, https://www.insurancejournal.com/news/east/2021/05/06/612996.htm.

Bromley P, Powell WW (2012) From smoke and mirrors to walking the talk: Decoupling in the contemporary world. *Academy of Management Annals* 6(1):483-530.

Bruynseels L, Cardinaels E (2014) The audit committee: Management watchdog or personal friend of the CEO? *The Accounting Review* 89(1):113-145 Article.

Center for Audit Quality, Deloitte (2022) Audit committee practices report: Common threads across audit committees.

Chen X, Cheng Q, Wang X (2015) Does increased board independence reduce earnings management? Evidence from recent regulatory reforms. *Review of Accounting Studies* 20(2):899-933.

Cheng JY-J, Groysberg B, Healy P, Vijayaraghavan R (2021) Directors' perceptions of board effectiveness and internal operations. *Management Science* 67(10):6399-6420.

Clune R, Hermanson DR, Tompkins JG, Ye Z (2014) The nominating committee process: A qualitative examination of board independence and formalization. *Contemporary Accounting Research* 31(3):748-786.

Cohen JR, Krishnamoorthy G, Wright AM (2002) Corporate Governance and the Audit Process. *Contemporary Accounting Research* 19(4):573-594 https://doi.org/10.1506/983M-EPXG-4Y0R-J9YK.

--- (2008a) The corporate governance mosaic and financial reporting quality. *Journal of Accounting Literature*:87-152.
--- (2008b) Form versus substance: The implications for auditing practice and research of alternative perspectives on corporate governance. *Auditing: A Journal of Practice & Theory* 27(2):181-198.
--- (2010) Corporate governance in the post-Sarbanes-Oxley era: Auditors' experiences. *Contemporary Accounting Research* 27(3):751-786.
--- (2017) Enterprise risk management and the financial reporting process: The experiences of audit committee members, CFOs, and external auditors. *Contemporary Accounting Research* 34(2):1178-1209.
Cohen JR, Hoitash U, Krishnamoorthy G, Wright AM (2014) The effect of audit committee industry expertise on monitoring the financial reporting process. *The Accounting Review* 89(1):243-273 Article.
Couchoux O (2023) Navigating knowledge and ignorance in the boardroom: A study of audit committee members' oversight styles. *Contemporary Accounting Research* Forthcoming.
Council of Institutional Investors (CII) (2016) Prioritizing cybersecurity. Report.
Cybersecurity Disclosure Act of 2021. (2021) In *S.808*, edited by Congress US: U.S. Congress.
DeFond ML, Hann RN, Xuesong HU (2005) Does the market value financial expertise on audit committees of boards of directors? *Journal of Accounting Research* 43(2):153-193 Article.
DiMaggio PJ, Powell WW (1983) The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. *American Sociological Review* 48(2):147-160.
Doan M (2019) Companies need to rethink what cybersecurity leadership is. November 27, 2019, https://hbr.org/2019/11/companies-need-to-rethink-what-cybersecurity-leadership-is.
Dodgson MK, Agoglia CP, Bennett GB, Cohen JR (2020) Managing the auditor-client relationship through partner rotations: The experiences of audit firm partners. *The Accounting Review* 95(2):89-111 Article.
Duchin R, Matsusaka JG, Ozbas O (2010) When are outside directors effective? *Journal of Financial Economics* 96(2):195-214.
Edmans A, Gosling T, Jenter D (2023) CEO compensation: Evidence from the field. *Journal of Financial Economics* 150(3):103718-undefined.
Eisenhardt KM (1989) Agency theory: An assessment and review. *Academy of Management Review* 14(1):57-74.
Faleye O, Hoitash R, Hoitash U (2011) The costs of intense board monitoring. *Journal of Financial Economics* 101(1):160-181.
Fama EF (1980) Agency problems and the theory of the firm. *Journal of Political Economy* 88(2):288-307.
Fama EF, Jensen MC (1983) Separation of ownership and control. *Journal of Law and Economics* 26(2):301-325.
Federal Trade Commission (FTC) (2021) Corporate boards: Don't underestimate your role in data security oversight. edited by Ho J. Washington, D.C.
Ferracone. (2019) Good governance: Do boards need cyber security experts? *Forbes*. Forbes, Accessed October 5, 2021, https://www.forbes.com/sites/robinferracone/2019/07/09/good-governance-do-boards-need-cyber-security-experts/?sh=15d506f21859.
Fich EM, Shivdasani A (2007) Financial fraud, director reputation, and shareholder wealth. *Journal of Financial Economics* 86(2):306-336.
Fisher RJ (1993) Social desirability bias and the validity of indirect questioning. *Journal of Consumer Research* 20(2):303-315.
Fox J (2021) Cybersecurity Statistics for 2021. February 28, 2021, https://cobalt.io/blog/cybersecurity-statistics-2021.
Free C, Trotman AJ, Trotman KT (2021) How Audit Committee Chairs Address Information-Processing Barriers. *Accounting Review* 96(1):147-169 Article.
Gartner (2021) Forecast: Information security and risk management, worldwide, 2019-2025, 1Q21 update. https://www.gartner.com/document/3999995.

Gendron Y, Bédard J (2006) On the constitution of audit committee effectiveness. *Accounting, Organizations and Society* 31(3):211-239.
Goh BW (2009) Audit committees, boards of directors, and remediation of material weaknesses in internal control. *Contemporary Accounting Research* 26(2):549-579 Article.
Hambrick DC, Misangyi VF, Park CA (2015) The quad model for identifying a corporate director's potential for effective monitoring: Toward a new theory of board sufficiency. *Academy of Management Review* 40(3):323-344 Article.
Hayne C, Vance M (2019) Information intermediary or de facto standard setter? Field evidence on the indirect and direct influence of proxy advisors. *Journal of Accounting Research* 57(4):969-1011.
Hermanson DR, Hurley PJ, Obermire KM (2023) Audit Committee Research: Where Do We Stand, and Where Do We Go from Here? *AUDITING: A Journal of Practice & Theory*:1-21.
Hermanson DR, Tompkins JG, Veliyath R, Ye Z (2012) The compensation committee process. *Contemporary Accounting Research* 29(3):666-709 Article.
Hillman AJ, Dalziel T (2003) Boards of directors and firm performance: Integrating agency and resource dependence perspectives. *Academy of Management Review* 28(3):383-396.
Hoitash U, Hoitash R, Bedard JC (2009) Corporate governance and internal control over financial reporting: A comparison of regulatory regimes. *The Accounting Review* 84(3):839-867.
Holder-Webb L, Cohen JR, Nath L, Wood D (2009) The Supply of Corporate Social Responsibility Disclosures Among U.S. Firms: JBE. *Journal of Business Ethics* 84(4):497-527.
Huang HH, Wang C (2021) Do banks price firms' data breaches? *The Accounting Review* 96(3):261-286 Article.
Hwang B-H, Kim S (2009) It pays to have friends. *Journal of Financial Economics* 93(1):138-158.
Institute of Internal Auditors (IIA). 2010. "Global technology audit guide (GTAG(R)) 15 information security guidance." edited by Love P, Reinhard J, Schwab AJ, Spafford G. Altamonte Springs, FL: Institute of Internal Auditors. https://www.iiacolombia.com/resource/guias/GTAG15.pdf.
Internet Security Alliance (ISA), National Association of Corporate Directors (NACD) (2020) Internet Security Alliance and National Association of Corporate Directors Release New Guide for Cyber-Risk Oversight. Arlington, VA: Internet Security Alliance.
Jackson RJ (2018) Speech: Corporate governance: On the front lines of America's cyber war. edited by Securities and Exchange Commission.
Jensen MC (1993) The modern industrial revolution, exit, and the failure of internal control systems. *Journal of Finance* 48(3):831-880 Article.
Jensen MC, Meckling WH (1976) Theory of the firm: Managerial behavior, agency costs and ownership structure. *Journal of Financial Economics* 3(4):305-360.
Johns G (2006) The Essential Impact of Context on Organizational Behavior. *Academy of Management Review* 31(2):386-408.
--- (2017) Reflections on the 2016 Decade Award: Incorporating Context in Organizational Research. *Academy of Management Review* 42(4):577-595.
Kalbers LP, Fogarty TJ (1998) Organizational and economic explanations of audit committee oversight. *Journal of Managerial Issues*:129-150.
Kamiya S, Kang J-K, Kim J, Milidonis A, Stulz RM (2021) Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics* 139(3):719-749.
Kang YJ, Trotman AJ, Trotman KT (2015) The effect of an Audit Judgment Rule on audit committee members' professional skepticism: The case of accounting estimates. *Accounting, Organizations and Society* 46:59-76.
Klein A (2002) Audit committee, board of director characteristics, and earnings management. *Journal of Accounting and Economics* 33(3):375-400.
KPMG (2021) Views from the boardroom: 2021 pulse survey. Report.
Krishnan J (2005) Audit committee quality and internal control: An empirical analysis. *The Accounting Review* 80(2):649-675.

Krishnan J, Wen Y, Zhao W (2011) Legal Expertise on Corporate Audit Committees and Financial Reporting Quality. *The Accounting Review* 86(6):2099-2130.
Larcker DF, Reiss PC, Tayan B (2017) Critical update needed: Cybersecurity expertise in the boardroom. *Rock Center for Corporate Governance at Stanford University Closer Look Series: Topics, Issues and Controversies in Corporate Governance No. CGRP-69*:17-70.
Lee AS, Baskerville RL (2003) Generalizing Generalizability in Information Systems Research. *Information Systems Research* 14(3):221-243.
Lisic LL, Myers LA, Seidel TA, Zhou J (2019) Does audit committee accounting expertise help to promote audit quality? Evidence from auditor reporting of internal control weaknesses. *Contemporary Accounting Research* 36(4):2521-2553.
Lowry MR, Sahin Z, Vance A (2022) Taking a Seat at the Table: The Quest for CISO Legitimacy. Systems AfI, ed. *ICIS 2022 Proceedings*.
Malsch B, Salterio SE (2016) "Doing good field research": Assessing the quality of audit field research. *Auditing: A Journal of Practice & Theory* 35(1):1-22 Article.
Masulis RW, Mobbs S (2014) Independent director incentives: Where do talented directors spend their limited time and energy? *Journal of Financial Economics* 111(2):406-429.
McDaniel L, Martin RD, Maines LA (2002) Evaluating financial reporting quality: The effects of financial expertise vs. financial literacy. *The Accounting Review* 77(s-1):139-167.
Miles MB, Huberman AM, Saldaña J (2020) *Qualitative Data Analysis: A Methods Sourcebook*, 4th Edition ed. (Sage Publications, Thousand Oaks, CA).
Milica L, Pearlson K (2023) Boards are having the wrong conversations about cybersecurity. *Harvard Business Review*.
Morgan S (2019) Global cybersecurity spending predicted to exceed $1 trillion form 2017-2021. *Cybercrime Magazine*.
Morse JM (1995) The significance of saturation. *Qualitative Health Research* 5(2):147-149.
Mullins F (2018) HR on board! The implications of human resource expertise on boards of directors for diversity management. *Human Resource Management* 57(5):1127-1143 https://doi.org/10.1002/hrm.21896.
Myers MD (2009) *Qualitative Research in Business & Management* (Sage Publications Ltd., Thousand Oaks, CA).
National Association of Corporate Directors (NACD) (2018) 2018-2019 NACD Public Company Governance Survey. Report, Arlington, VA.
--- (2020) Cyber-risk oversight 2020: Key principles and practical guidance for corporate boards. National Association of Corporate Directors (NACD), Internet Security Alliance, eds.
New York Department of Financial Services (2017) Cybersecurity requirements for financial services companies. In *23 NYCRR s 500.4(b)*.
NYDFS (2023) Cybersecurity requirements for financial services companies: Second amendment to 23 NYCRR 500. In *23*, edited by New York State Department of Financial Services.
Odendahl T, Shaw AM (2002) Interviewing Elites. Gubrium JF, Holstein JA, eds. *Handbook of Interview Research: Context and Method* (Sage Publications, Thousand Oaks, CA), 299-316.
Paternoster R, Simpson S (1996) Sanction threats and appeals to morality: Testing a rational choice model of corporate crime. *Law and Society Review* 30(3):549-583.
PCAOB (2018) Panel discussion: Cybersecurity. In *Standing Advisory Group Meeting*, edited by Public Company Accounting Oversight Board. Washington, DC: PCAOB.
Perullo J (2021) Cybersecurity in the three lines model. December 27, 2021, https://www.linkedin.com/pulse/cybersecurity-three-lines-model-jerry-perullo/.
Piquero AR, Bouffard JA, Piquero NL, Craig JM (2016) Does morality condition the deterrent effect of perceived certainty among incarcerated felons? *Crime & Delinquency* 62(1):3-25.
PwC (2019) PwC's 2019 Annual Corporate Directors Survey. Report.

--- (2021) Stronger enforcement puts teeth in cyber and privacy rules. June 21, 2021, https://www.pwc.com/us/en/services/consulting/cybersecurity-privacy-forensics/library/cybersecurity-enforcement-financial-sector.html.
--- (2022) Overseeing cyber risk: The board's role. Report.
Rundle J (2023) Boards Still Lack Cybersecurity Expertise; Just 12% of S&P 500 companies have board directors with relevant cyber credentials, new study says. *Wall Street Journal (Online)* (09/25/ 2023 Sep 25), https://www.wsj.com/articles/boards-still-lack-cybersecurity-expertise-70094266.
Saldaña J (2013) *The Coding Manual for Qualitative Researchers*, Second ed. (Sage Publications).
Schwartz-Ziv M, Weisbach MS (2013) What do boards really do? Evidence from minutes of board meetings. *Journal of Financial Economics* 108(2):349-366 Article.
SEC (2011) Cybersecurity. In *SEC Division of Corporation Finance*, edited by Securities and Exchange Commission. Washington D.C.: SEC.
--- (2018) Commission Statement and Guidance on Public Company Cybersecurity Disclosures. edited by Securities and Exchange Commission. Washington, D.C.: SEC.
--- (2021a) SEC charges Pearson Plc for misleading investors about cyber breach. In *2021-154*. Washington, D.C.: Securities and Exchange Commission.
--- (2021b) SEC announces three actions charging deficient cybersecurity procedures. In *2021-169*. Washington, D.C.: Securities and Exchange Commission.
--- (2021c) Cybersecurity Risk Governance. edited by Securities and Exchange Commission. Washington, D.C.
--- (2021d) SEC charges issuer with cybersecurity disclosure controls failures. In *2021-102*. Washington, D.C.: Securities and Exchange Commission.
--- (2022) Proposed Rule: Cybersecurity Risk Management, Strategy, Governance and Incident Disclosure. Washington, DC: Securities and Exchange Commission.
--- (2023) Final Rule: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure. In *Release No. 33-11216*, edited by Securities and Exchange Commission. Washington, D.C.: SEC.
Sila V, Gonzalez A, Hagendorff J (2017) Independent director reputation incentives and stock price informativeness. *Journal of Corporate Finance* 47:219-235.
Suchman MC (1995) Managing Legitimacy: Strategic and Institutional Approaches. *The Academy of Management Review* 20(3):571-610.
Tidy J (2021) U.S. companies hit by 'colossal' cyberattack. *BBC News*, July 3, 2021, https://www.bbc.com/news/world-us-canada-57703836.
Trotman AJ, Trotman KT (2015) Internal audit's role in GHG emissions and energy reporting: Evidence from audit committees, senior accountants, and internal auditors. *Auditing: A Journal of Practice & Theory* 34(1):199-230.
Tunggal AT (2021) Why is cybersecurity important. *Cybersecurity*, July 1, 2021, https://www.upguard.com/blog/cybersecurity-important.
Tuttle B, Dillard J (2007) Beyond competition: Institutional isomorphism in US accounting research. *Accounting Horizons* 21(4):387-409.
U.S. Department of the Treasury (2001) Interagency Guidelines Establishing Standards for Safeguarding Customer Information and Recision of Year 2000 Standards for Safety and Soundness. edited by Department of the Treasury.
--- (2020) Consent Order In *AA-EC-20-49*, edited by Department of the Treasury. Washington, D.C.: U.S. Department of the Treasury, Office of the Comptroller of the Currency.
Weisbach MS (1988) Outside directors and CEO turnover. *Journal of Financial Economics* 20:431-460.
Wijen F (2014) Means versus Ends in Opaque Institutional Fields: Trading off Compliance and Achievement in Sustainability Standard Adoption. *Academy of Management Review* 39(3):302-323.
Xie B, Davidson WN, DaDalt PJ (2003) Earnings management and corporate governance: The role of the board and the audit committee. *Journal of Corporate Finance* 9(3):295-316.

Yin RK (2018) *Case Study Research and Applications: Design and Methods*, 6th Edition ed. (SAGE Publications, Inc., Los Angeles, California).

Table 1 Interview Details

Panel A: Director interview details

Interview #	Interview length (min)	Committee participation related to cybersecurity	# of positions	Years of director experience	Years at current largest firm	Cyber expertise	Experience in technical executive position (years)	Market Cap (P-private firm)	Represented industries
D-1	53	Audit (chair)	3	14	1	No	n/a	Mid	Wholesale trade Retail trade Services
D-2	50	Audit (member)	4	20	20	No	n/a	Large	Manufacturing Wholesale trade
D-3	67	Audit (chair)	2	6	6	No	n/a	Mid	Financial services Manufacturing
D-4	63	Audit (member)	2	17	8	No	n/a	Mid	Services
D-5	49	Audit (member)	2	7	2	Yes	18	Mid (P)	Services
D-6	62	Audit (chair, member)	3	18	15	No	n/a	Large	Construction Financial services
D-7	63	None	3	12	12	No	n/a	Mid	Manufacturing Retail trade Financial services
D-8	55	Audit (member)	1	4	4	No	n/a	Mid	Services
D-9	32	None	1	9	9	Yes	12	Mid (P)	Services
D-10	43	Audit (member), Risk (member)	6	16	8	No	n/a	Mid	Services Financial services
D-11	32	Audit (member)	7	9	2	Yes	5	Mid	Services Financial services
D-12	53	Audit (member)	2	6	6	Yes	17	Large	Services Medical
D-13	46	Audit (member)	1	4	4	Yes	5	Mid	Mining
D-14	61	Audit (member)	3	14	14	No	n/a	Large	Manufacturing
D-15	54	Audit (member)	4	15	11	No	n/a	Small	Retail trade
D-16	41	Audit (member)	2	3	3	No	n/a	Large	Manufacturing Services
D-17	52	Audit (chair)	3	17	3	No	n/a	Small	Manufacturing Services

D-18	37	Executive director and CFO	1	12	12	No	n/a	Small	Retail trade
D-19	51	Risk (member)	3	4	4	No	n/a	Small	Financial services
D-20	40	Audit (member)	2	2	2	No	n/a	Large	Manufacturing Financial services

Panel B: Executive interview details

Interview #	Position	Interview length (min)	Years of experience as head of security	Years of experience at current position	Market Cap	Represented industries
E-1	CIO	52	27	13	Mid	Wholesale trade
E-2	CISO	66	20	2	Mid (P)	Services
E-3	CISO	60	13	2	Mid (P)	Financial services
E-4	CISO	46	7	7	Large (P)	Transportation & public utilities
E-5	CISO	61	6	6	Mid (P)	Services
E-6	CISO	63	23	9	Large	Financial services
E-7	CISO	63	21	1	Large	Manufacturing, services
E-8	CSO	63	33	33	Large	Manufacturing
E-9	CISO	54	33	5	Large	Wholesale trade
E-10	CISO	37	6	6	Small	Retail trade
E-11	CIO	51	20	3	Large	Manufacturing

Panel C: Consultant interview details

Interview #	Interview length (min)	Position	Years of consulting experience	Type of consulting firm
C-1	45	Distinguished engineer	37	Technology solutions firm
C-2	50	Managing director	18	Big-4 accounting firm
C-3	48	Executive	5	Cybersecurity risk ratings firm
C-4	80	Founder/CEO	23	Risk management consulting firm
C-5	84	Founder/CEO	2	Risk management consulting firm
C-6	67	Partner	17	Big-4 accounting firm
C-7	76	Director	18	Big-4 accounting firm

Panel A presents director participants and the firms they represent. The number of director positions reflects corporate director positions within five years of their interviews. Cybersecurity expertise is based on directors' self-disclosure and verification based on their work history. With the exception of D-9 and D-18 who were executive directors, all directors were independent directors. Market capitalization ranges are: Mid-cap, $2-9.9 billion; Large-cap, $10+ billion, based on the director's largest firm, if publicly listed, or value upon privatization or annual revenues, if a private firm.

Table 2: The Role of Expertise in Director Questioning of CISOs

Panel A: Summary of views by participant category

Is director questioning substantially affected by cybersecurity expertise?	Nonexpert		Director Experts		Executive/ Consultant Experts	
	N	%	N	%	N	%
Yes	3	23.1%	5	100.0%	12	92.3%
No	8	61.5%	0	0.0%	0	0.0%
Mixed	2	15.4%	0	0.0%	1	7.7%

Panel B: Representative quotes

Questioning is substantially affected by expertise - Agree
[T]he number of [board members] who have hands-on expertise enough to comprehend the cyber issues in detail and ask the kinds of questions a board member typically is capable of asking a CFO—about cashflow, about lending instruments, about credit risk, about the variety of common oversight type issues, days receivable outstanding, and the things that leap off of a page that a good board can provide good governance about—there's no analog for cyber. (D-9 expert)
Well, if they have any expertise in the area, …they're going to ask intelligent questions. (D-12 expert)
Questioning is substantially affected by expertise - Disagree
I cannot imagine asking any more questions than either I've asked personally, or my colleagues have asked about [cybersecurity]. (D-3 nonexpert)
I've not noticed [a difference in question quality]. It's not to the degree where we're just relying on [the expert director] to come up with the questions. I think, because just the nature of our oversight, everyone's participating, asking questions. I don't see her questions are different than anybody else's questions. (D-16 nonexpert)

This table presents participant views on the role of expertise in director questioning by participant type. Panel A presents a summary of participant views on whether director questioning is substantially affected by cybersecurity expertise. Two authors coded each participants' stance as essentially agree, disagree, mixed or silent, and differences were reconciled. Panel B presents representative quotes underlying this coding.

Table 3 Perceptions of CISO Filtering

Panel A: Summary of views by participant category

Is CISO filtering a concern?	Nonexpert		Director Experts		Executive/ Consultant Experts	
	N	%	N	%	N	%
Yes	5	38.5%	4	80.0%	12	75.0%
No	6	46.2%	0	0.0%	4	25.0%
Mixed	2	15.4%	1	20.0%	0	0.0%

Panel B: Representative comment quotes

CISO filtering is a concern - Agree
I think there's always that risk and I think that a board should have a high awareness and concern for that. (D-5 expert)
[In response to whether CISOs take advantage of board's low expertise to filter reports] For sure, of course, all of the time. If you look at any of the board briefings that I've seen, they are not helpful. They're either intended to be at such a high level of abstraction that the board can't get into their knickers. Or alternatively, they are so geeked up that the board can't understand it. (D-12 expert)
CISO filtering is a concern - Disagree
I don't see it….The CISO appears in front of the board periodically with an external auditor so I just don't know whose advantage it would be. So what if the auditor finds something bad and they need to assess some things, why wouldn't the CISO use that as an advantage to get some money for the investments? (D-2 nonexpert)
They're not trying to hide things. If they're any good, that is not their DNA. They are, the closest thing I can say, they're a lot like an internal auditor. They understand that there will always be work to be done. And so, a high-performing CISO I think sees no incentive. (D-10 nonexpert)

This table presents participant views on CISO filtering by participant type. Panel A presents a summary of participant views on whether CISO filtering was a concern in cybersecurity risk oversight. Two authors coded each participants' stance as essentially agree, disagree, mixed or silent, and differences were reconciled. Panel B presents representative quotes underlying this coding.

Table 4: Is Expertise Needed?

Panel A: Summary of views by participant category

Is expertise needed for effective cybersecurity risk oversight?	Nonexpert		Director Experts		Executive/ Consultant Experts	
	N	%	N	%	N	%
Yes	5	33.3%	4	80.0%	12	75.0%
No	8	53.3%	0	0.0%	1	6.3%
Mixed/No clear stance	2	13.3%	1	20.0%	3	18.8%

Panel B: Representative comment quotes

Expertise is needed for cybersecurity oversight - Agree
[In response to question about advice to boards on how to effectively oversee cybersecurity] Mak[e] sure you have the level of expertise of a board member that can ask the really hard questions and you need a translator….[in my deep dive] I was able to give them some advice and things that they should think about. (D-5 expert)
I think that boards and companies should be smart enough to know, this is an area that [companies] are exposed in. [Companies] should find somebody that actually knows something about this and bring them on the board. (D-11 expert)
Expertise is needed for cybersecurity oversight - Disagree
[Assessing their board's ability to provide cybersecurity risk oversight, despite the board not having expertise] I don't think we're any different than anybody else. I think we have adequate coverage. (D-6 nonexpert)
Having the expertise will never be a negative thing, okay? So that's obvious, but to make it an absolute criteria, I'm not sure that's needed. … I don't think that you need to have that cyber expert person on the board in order to operate efficiently. (D-20 nonexpert)

This table presents participant views on the need for board-level cybersecurity expertise by participant type. Panel A presents a summary of participant views on whether cybersecurity expertise is needed for effective cybersecurity risk oversight. Two authors coded each participants' stance as essentially agree, disagree, mixed or silent, and differences were reconciled. Panel B presents representative quotes underlying this coding.

Appendix A. Sample of Questions from Semi-Structured Interviews

Note: *Below are sample questions from our semi-structured interviews. Given the semi-structured nature of the interviews, these questions represent starting points for discussion. The interview script was customized according to the interviewee's role (i.e., director, executive, or consultant) and relevant background.*

What does "cybersecurity risk" mean to you?

- Do you think that it would be defined in the same way by the directors on your boards?
- [If mentions challenges of cybersecurity] Can you speak to how the unique challenges related to cybersecurity cause your board to approach this risk differently from other enterprise risks?

Outside of the board, who are the other major players with respect to cybersecurity risk management?

- Who provides oversight over these individuals and/or departments that are responsible for cybersecurity risk?
- Within the board, is oversight shared between committees or between the main board and committees?
- For those not on the audit/enterprise risk committee, do they also have responsibility for cybersecurity oversight? If so, what does cybersecurity oversight entail for them?

We would like you to think about the last four board meetings. How was cybersecurity covered, if at all?

Overall, how would you characterize the board's level of experience with cybersecurity issues?

- Can you describe how an individual board member's level of experience impacts how they provide cybersecurity oversight? [Can you give us any examples?]
- How does a given board member's experience with cybersecurity impact the priority they place on cybersecurity oversight?
- How do board members educate themselves about cybersecurity?
- Do you think the board has enough expertise in cybersecurity to provide effective oversight for this risk? Why (why not)?
- Can you describe any challenges from overseeing management (e.g., CISO, CIO) with relatively more experience in cybersecurity?

Can you briefly talk about any cybersecurity consulting engagements [in the case of a consultant interviewee: your practice provides] that involve oversight at the board level?

Overall, how would you rate the board's effectiveness in cybersecurity risk oversight?

Does management have any incentive to filter the reports they give to the board?

Is there any advice you would give to another board on how to effectively oversee cybersecurity?

Is there anything you thought we would ask but we didn't, or is there anything else you would like to tell us?

Appendix B: SEC Cybersecurity Proposed Rule on Expertise Disclosure

Release Nos. 33-11038; 34-94382; IC-34529; File No. S7-09-22]

This table presents a summary of 191 SEC comment letters regarding the SEC's 2022 proposed cybersecurity rules. Two research assistants performed the initial coding under the guidance of one of the authors, then any differences were reconciled by one the authors. Another coauthor was brought in for consultation for any cases where there was ambiguity. We find that 43 percent of all comment letters discussed the proposed rule of board expertise disclosure, and that the comment letters present similar variations in views as our participants regarding director cybersecurity expertise., Just About one-third of such discussions were in favor of the disclosure. Objections included a concern that requiring disclosure would create a de facto expectation for director cybersecurity expertise, that such cybersecurity expert directors may not be able to contribute to the board for the wide range of board duties, that there is a scarcity of expertise in the director pool and in particular that small firms could not compete for skilled directors. Comment letters also cited that directors could lean on management and outside experts. Thus, objections focused on the costs and logistical issues for firms who may want to secure cybersecurity expertise, and our findings that director expertise in cybersecurity leads to more substantive oversight provides insight into the benefits of obtaining expertise. The comment letters also raised concerns regarding how to define cybersecurity expertise.

Table B1: SEC Cybersecurity Proposed Rules

Panel A: Summary of comment letter categorization

Total Comment Letters	191	
Comment Letters that discuss disclosure of director expertise	83	
Comments in favor of disclosure of director expertise	27	32.5%
Comments against disclosure of director expertise	48	57.8%
Other comment on disclosure of director expertise	8	9.6%
Total	83	100.0%

Table B1: SEC Cybersecurity Proposed Rules (cont.)

Release Nos. 33-11038; 34-94382; IC-34529; File No. S7-09-22]

Panel B: Representative comment quotes

Comments in favor of disclosure of director expertise
The SANS Institute believes that cyber expertise is needed on the board of public corporations. The expertise should focus on cyber implications with directors who understand these issues. The SANS Institute believes this is possible through proper training and certifications that validate directors' skills, similar to other industries, such as an accountant that has achieved their Certified Public Accountant designation. This will give confidence to the investors and assurance that the board can make smart decisions concerning cyber risk and investments. *The SANS Institute*
We have consistently supported legislative efforts to require publicly traded companies to disclose in their annual reports or annual proxy statements, whether any member of their governing body, such as a board of directors, has expertise or experience in cybersecurity issues. .....Beyond supporting cybersecurity strategies that address internal company-related risks, ensuring board members' understanding of the cybersecurity landscape is also vital to their understanding of external company-related risks. ...The board should be comprised of skilled directors with a balance of broad business experience and extensive industry expertise to understand and question the breadth of risks faced by the company. Risks posed by cybersecurity incidents and threats should be understood by board members, and we have long advocated that board members should develop and have cybersecurity expertise. *CEO of CALPERS*
We are pleased to see that the Proposed Rules address the role of the board in cybersecurity risk management and strategy in a thorough manner, including disclosure of whether any board member has expertise or experience in cybersecurity. ...We believe disclosing the names of board members with cyber expertise is unlikely to deter such members from performing board service. These skills are highly sought after, ...We believe that annual disclosure of cyber expertise among board members, if any, in the annual report and proxy would be helpful to investors, especially in voting decisions. *Council of Institutional Investors*
One effective regulatory approach would be asking public companies to disclose whether a cybersecurity expert is on the board of directors, and if not, why not. We have sponsored bipartisan legislation called the Cybersecurity Disclosure Act to require companies to provide this disclosure to investors. *United States Senators Jack Reed, Mark R. Warner, Catherine Cortez Masto, Kevin Cramer, Susan M. Collins, Angus S. King, Jr., and Ron Wyden*
Comments against disclosure of director expertise
Against de facto mandate, scarcity of talent, disproportionate effect on small firms Although these proposed amendments do not *mandate* that corporate boards include a member with expertise in cybersecurity, they have the implicit suggestion that corporate boards *should* include a member with such qualifications. Failure to have a board member with expertise in cybersecurity, therefore, could result in investors reaching the mistaken conclusion that a company is unconcerned with cybersecurity. While the Exchange agrees with the Commission that cybersecurity is an important area of focus for nearly all public companies, it does not believe that the absence of a cybersecurity expert on a company's board is necessarily the fatal flaw that the required disclosure may implicitly suggest to investors. … In the area of cybersecurity, a corporate board may rely on reporting from an in-house cybersecurity team or external consultants. Relying on non-board member experts should not suggest that a company is unserious about cybersecurity. ...If the Proposal is adopted in its current form, the Exchange believes that many companies will prioritize attracting board members with "cybersecurity expertise" in order to demonstrate their commitment to managing cybersecurity risk. With 7,848 companies filing on domestic forms and 973 FPIs filing on foreign forms during calendar year 2020, the NYSE questions whether there are truly enough individuals with both cybersecurity expertise and other relevant experience to make them suitable candidates for service on a corporate board. If a shortage does exist, the Exchange is also concerned that smaller and medium-sized companies may be disproportionately disadvantaged in attracting these highly sought after individuals for board service. *NYSE Group*

Scarcity of talent [T]he NACD Cyber-risk Oversight handbook 2020 observes "there simply are not enough 'cyber experts' to populate every board." ...The NACD's Governing Digital Transformation: A Practical Guide similarly points out that a common pitfall of recruiting "digital directors" is focusing solely on individuals with technical backgrounds because other skills and backgrounds might be more useful from a governance perspective. Thus, whether a board includes a cybersecurity expert might not be as relevant as the other proposed disclosures related to cybersecurity governance (for example, proposed Item 106(c) of Regulation S-K). The SEC might instead consider revising the Proposal to elicit disclosure of how or whether the board engages with experts to execute its governance role over cybersecurity. Such a disclosure would complement the proposed disclosures in Item 106(c) while providing registrants with the flexibility needed to craft cybersecurity governance appropriate to their organization. *Crowe LLC*
De facto mandate, scarcity of talent, one trick ponies, director education and relying on management is sufficient The requirement to disclose whether the issuer has a cybersecurity expert on the Board of Directors could evolve into a market expectation that all issuers have an expert on their Board. PPG does not believe that the Commission's disclosure rules should be a "de facto" governance requirement. ... the requirements of proposed Item 407(j) are so specific that there likely is not a large pool of director candidates with this level of expertise who also have the general leadership and business experience to serve as a director of a public company. Directors can gain expertise on cybersecurity (or many other company risks) through educational opportunities, table-top exercises and from the issuer's own cybersecurity team. Issuers would be better served having a cybersecurity expert with the qualifications set forth in proposed Item 407(j) on their management team, rather than on the Board. *PPG Industries, Inc.*
De facto mandate, current rules are sufficient We believe dedicated expertise may be valuable for some companies. In general, however, especially given the limited size of boards, it may not be practical or advisable for a board to recruit dedicated experts in each of its critical oversight areas. While we recognize that neither of the proposals requires designated board experts, we believe that, especially when read together, some may infer that the Commission prefers that issuers identify such experts. We therefore encourage the Commission to consider whether existing proxy rules (which require disclosure of the particular experience, qualifications, attributes, or skills of board nominees), when combined with disclosure regarding board oversight of a company's cybersecurity risk, may be sufficient to inform investors about the role of the board in cyber risk management, without a separate requirement to identify cybersecurity experts. *Deloitte & Touche LLP*

Appendix C: Additional Interview Evidence

Table C1: Additional Interview Evidence of How Expertise Affects Boards' Cybersecurity Oversight

4.2. How expertise influences board engagement
[B]oard members want to be useful. They want to make the company successful and therefore, they are inclined to speak more about it and dwell on things where they feel like they can contribute. (D-9 expert) Yeah, because your general board members, because they have their day life and whatever is exacting or commanding their attention in the course of any given week, may not have time to dabble in paradigm battles… And to even be positioned to even have the thought or to have it occur to you to even raise the implications of these emergent technologies, is probably not something a board member whose principal interests lie elsewhere, would have had the time to have even become aware that there's a question out there that you might want to pose or ask. (E-7) [T]he board should make sure it's got its governance structure right…. And if they do get that right, it has real world effects. Because then there's somebody on the board who is knowledgeable about cyber, and that means that the CISO has somebody to talk to. And there should be a line of communication between that board member and the CISO. And usually, that also means that the CISO gets out from under the CIO, doesn't report to the CIO directly. So, if you get the governance model right, these issues are going to get better funding and then get more time and attention. (C-3) [Without a director with expertise,] I would predict that there wouldn't have been somebody in the audit and finance committee who would've stepped up, because they're already busy. They got a lot to do. I would bet that somebody else, one of the other board members, would've asked the question …, "So what are you guys doing about cybersecurity?" We would've had to go in and present, but it would've been at a much higher level. [Without the director with expertise] I don't know that we ever would've had this maturity model in place. … [C]ertainly we wouldn't have done that third party review and bring that in.… I think we would be at a very different [level]... I think it took an IT person to be able to really drill in and understand at the level she wanted to. I don't think the others would just have the interest. They would just want to know it's protected, and, "Do you have somebody in charge of it," or, "Do they know what they're doing," kind of thing. (E-2) [T]he audit committee chair said, "I would like to do a benchmark and analysis using the same yardstick, the same measuring stick, to see how one [company] stacks up against the other, where we're strong, where we're weak, where there's synergies, where there's big gaps." And that launched our whole project. …Oftentimes, that is where it comes, is at the request of one board member who is seen as the IT or cybersecurity expert who can ask for those special things that sends the CISO or the CIO, or the chief risk officer, or the chief legal officer off to do these reports or these sorts of analyses. (C-7) I'm the lead on cybersecurity risks. And just by the nature of my background, I work very closely with the other chair on setting cybersecurity goals and what the board should be focusing on. Along with the IT leadership, we have inter-quarter calls …checking on how things are going, whether the board should be specifically looking at things that we were not aware of. And I help to interpret some of the technical language into risks for the board. (D-13 expert) I now meet with [the IT leadership] team on the off months that we do not have board meetings…we deep dive a myriad of issues. And the more you know, the more there is to know, which is pretty overwhelming.

And so we're just trying to get at, "what's most important to the board? How are we getting at risk? How are we looking at more specifically evaluating the risk of the crown jewels of the company?" (D-20 expert)

4.3 How expertise influences questioning

But [X, a director with more cyber expertise] just comes up with good ideas, good things to think about, or for management to think about. Not only just where do the ones and zeros go, but how are you structured, your organization? Where are you spending your time in your organization in your information areas? You know, your data processing areas and stuff. (D-1 nonexpert)

[Our more expert director] understands the ins and outs, and she's taken a liking to it. So she brings to the table a lot of things that we don't think about, and then she says, "Well, have you thought about this? Have you thought about that?" And that has been a godsend. (D-1 nonexpert)

People are quite diligent I've found on boards. They would typically spend the time and energy to get more knowledgeable and there are a lot of resources. And people on Boards, they're smart people. They know how to educate themselves. And what they do is they would do what I did. They would talk to other people, they would take courses, they would do whatever they needed to do to be sufficiently knowledgeable so that they can do the right thing. (D-1 nonexpert)

Most boards are filled with pretty smart people, and we're not afraid of not knowing what we don't know. We ask a lot of questions, and require that we get information….There are a lot of things that come before a board, where people around the board room table are not experts. However, most are seasoned business people. They ask the right questions, and their experience over time, they make sure that they get the right people in front of the board, to address the Q and A. On the cyber thing, as I said earlier, none of us have the millennial experience with these technology things, that are now called cyber risk. We have CIO's talk to us, we have their direct reports that are responsible for the cybersecurity, talk to the full board, and to the committees. Whether it is an issue, or a problem, I couldn't look you in the eye today, and say that that would be the case. (D-3 nonexpert)

[Director X] is probably our most versed person in his experience with these kinds of issues…. I know I wasn't brought in because of my cybersecurity expertise…. It's helpful to have someone who's kind of lived in the world on the front edge of things a little bit, and I think boards certainly would benefit by having somebody that has knowledge of what are the questions that need to be asked and the issues that need to be addressed so that you don't just get a kind of a glossy eye, 'we're on top of this and let us show you all the insurance we have to protect against all these different possibilities….' He just might ask more questions and have more insights than the average board member would... he tends to be someone who brings a little bit more to the party for that. (D-8 nonexpert)

I think, because just the nature of our oversight, everyone's participating, asking questions. I don't see [expert director's] questions are different than anybody else's question. I'm just trying to think back on some of the relevant conversations that we've had. Maybe. Maybe it's a little bit more technical than someone else's question, but it doesn't get real technical, if that makes sense. All of that conversation is something any board member would be able to understand the subject matter and the nature of the questions. (D-16 nonexpert)

[in contrast to cybersecurity] from an accounting standpoint, you can read the financial statements, you can see where the cash flows are coming form, you can see where the risks are. [In cybersecurity] you have to ask a bunch of questions and you need the background or knowledge of some of the technology to even be asking the question." D-18 nonexpert)

[In response to: Did they ask you any follow-up questions?] Nope. Which shows the maturity level of the board. They wouldn't be able to ask questions. (E-5) There's a language barrier here. Boards don't want to be embarrassed. They don't want to sit in a room and say, "What is that acronym," and, "What does that mean?" They're not going to do that. (C-6) That doesn't mean that they understand the answers, and that doesn't mean that they know what to do about it… So boards are getting smarter and smart enough to ask the questions. They're just not yet smart enough to interpret what the CISO is saying. (C-7)	
4.4. Lack of expertise requires coaching by CISOs	
Educating the board	The last presentation was to the full board, and they were just generally asking questions. A lot of them were generally asking questions about more, just trying to seek better understanding around cyber and what have you.... For a lot of the individuals, they were trying to still learn about cybersecurity. There were times where, especially right now with the ... different types of cyberattacks that are occurring, there's a certain level of interest to really understanding more. (E-3) One of the things that we implemented the first year I was here is a discipline, or I should say, a cadence where, at least once a year, we have a board education session. One year it was just security 101 kind of stuff. The anatomy of a program, how it's built, how you evolved to the strategy, how you execute, that kind of stuff. And then we did a tabletop demonstration, how we do our annual cybersecurity, executive tabletop exercises. We had one session on, 'How do you protect yourself from the criminal?' kind of thing. So every year we have that, and that's really helped in board education. (E-6) [T]he executive committee is essentially attending the audit committee meeting that I update in, which is great for me because it's a super opportunity not just to educate the board but [also] the executive committee and keep them in the loop. (E-9) We're bringing in the CISO to talk about what's going on. Part of that I would say is part of the governance, but also in terms of helping educate the directors. I mean, a lot of the directors are like me that grew up… When I was in [college] we were using punch cards for our computer science classes. (D-14 expert)
Conditioning the board	But we have really hammered that home, and this is the five functions that you align a cybersecurity program to. And this is the framework we're using to manage cybersecurity. So this is what one should look like, these are the things that you should have in place. And then we go through a process saying, "Well, this is the maturity of us against that framework of how we've implemented it." And then the rest of it becomes a little bit of trying to understand what's the best way to help them provide oversight, what are the best kind of reports. (E-3) [speaking as the CISO and their team] "(L)et us tell you what the risks are, let us tell you what we're most concerned about, and for those things we're concerned about we're going to report back to you on the progress we make on remediating that, and then... let me show you how we're protected from an insurance standpoint, too, so if something does go bump in the night, it's not going to harm the company's financial situation." (D-8 nonexpert)

	I took one of those [articles], "The Top 10 Questions Boards Should Ask CISOs." We took the questions, I filled it out, and then we just gave it to the board members and their repository to pre-answer before they ask. (E-6) Part of it starts with education. Explain to us what the risks are. And then, what are you doing to mitigate those? Probably, finally, how can we help? I mean, is it resources or investment? I think. It would be a combination of all of those things. (D-14 expert)
4.4 Expertise enables board members to challenge the CISO	
	In asking the CISO these questions, it was pretty clear the CISO was very old fashioned and was much more focused on keeping things out as opposed to assuming that people got in… And we ended up replacing that person. (D-11 expert) I think having people now on the boards that have that expertise is a risk mitigator for companies because it really is allowing subject matter expertise on the board to go. "We'll pull out here." [As an example of director feedback] "No, you're not making the right investment," or "You're not making the right level of investment." Or, "It's clear to me that the IT leadership in this company doesn't have the expertise needed to deal with the risks that are facing this company." And I think that's the value of having a board member that understands the cyber space. (E-8) [An expert director] said, "I'd like to see a third party brought in, somebody from the outside, to do an independent assessment of where you are from a cyber maturity perspective and then put together an initiative plan, so we understand where you're going and what things you're doing." So, we said, "All right." We wanted to proactively get in front of that. (E-2)
4.5 Expertise enables board members to detect false or withheld information	
	There is always a bit of "protect your house." We know that information is filtered to the board and that's why it's important to get outside sources of information…. [Regarding whether the filtering is unique to cybersecurity] I think it becomes more challenging because the boards may not know enough to ask as many questions. If you have a cyber expert it is probably not as big of an issue. It is more challenging because of the nature of it. …IT is a more dynamic thing that makes it more challenging. (C-2) [A director should be someone] who understands technology, who has done and overseen cybersecurity, so a former CIO, or a former CISO, somebody who has sat in the chair and has asked those questions of a CISO, or been in the operations seat and has done these things before. Otherwise, you run the risk of getting snowed, and you're going to." (C-6) [In response to how oversight is different if there is a board with expertise] Well, I mean, to be crude, to not get bullshitted in a meeting, right? So, if either one of you two are sitting in a meeting, a cyber meeting, and you see a board-level presentation, which is generally going to be fairly high level. But you're going to know the right kind of questions to start asking. You hear something in that presentation where it feels like, "Well, that feels a little weak," or "I'm not seeing something that I would expect to see in a cyber protection program here." …You bring somebody in, who's got real cyber expertise. I think that is a big risk mitigated for the board. (E-8) [In response to our question: Do they (CISOs) have pressure or incentive to provide a rosier picture, to make themselves look better or to make their boss look better?] Yeah, it's a great question. I think there's always the risk of that. This is where educating the board members to ask more piercing or penetrating questions and have their own expertise or having an expert on the board, I mean if you get

	to that point, helps. Part of it is that if there's an issue then you have to... Still doing the post-mortem of what happened. Why did this happen? What did we learn from it? There is some pressure. But, I think having the person in front of the board, you generally get a gauge in terms of the person is trying to just tell you a rosy picture or they're actually saying, "Here's a situation."

Table C2 Additional Interview Evidence of Whether Cybersecurity Expertise is Needed

Is cybersecurity expertise needed?	
Yes	[S]ome of our best practices in the industry are to add that cyber expert IT professional on the board. And that has been something that's been recent of the last three to five years, but a lot of focus the last two years…[we have] a spot, we don't have anyone who fills that now. I think that is a hole in our governance that we all recognize we need to do something about and put more internal focus on it….We should have cyber expertise I think on our boards …and the audit committee. We have GAAP, obviously, and we have all the rules and regulations around SOX that the financial statements stay true to intent. It seems like the way cyber is developing. it's right there, right behind financial statements right now. The integrity of the financial statements, the integrity of your systems and the reliability of your systems are one and two. (D-15 nonexpert) Having your own board member who is [themselves] an expert, in terms of the issues being discussed or presented, when the presenting CISO goes out of the room or looks away, [board members] can all look to you and say, "thumbs up?," ... [I]t's an extra little piece of validation, separate and independent of what their own personal entities might bring to the table. (E-7) [T]he board's chock full of all sorts of people who have run large businesses and understand governance and understand strategy and financial management systems and supply chains and all those things. And they're brought in because they had that experience. Why would you not do the same thing in your digitized space? Why wouldn't you bring somebody in that has that kind of expertise and knowledge, because in most corporations, that is the area where they are potentially the most singularly at risk for catastrophic failure. (E-8) I actually am very much an advocate of having a strong cyber presence on the board.… [T]here's virtually no industry that's untouched by [cybersecurity] anymore, and it's not going to get better in the short term. So I do support that approach and that regulation moving forward because I think the vast majority of boards are woefully—and this is from talking to peers and others—are inadequate in the space. I do support it. (E-9) It's an area that will be considered best practice today for a board to have expertise on and be a regular part of the communication at board meetings and regular updates. So it's not just SEC, but it's good business today. There's so many different ways that a company can be damaged. Everything from the stealing of critically important information, not even known as stolen. I think that becomes almost number one for a corporate. But of course, when you're being held hostage for a major payment and you're running a utility, it's pretty damn important as well. So the big problem that I see…is a shortage of expertise in the area and with a very high demand. (D-17 nonexpert)
Middle ground	I'd love to have more knowledge. I think having [Director X with expertise] come on the board helped. I think that having these third parties coming in every couple of years give you some validation of what's working and what's not working. I think it's a combination of a lot of things. Personally, I don't think you should get a board member that the only thing he or she brings to the board is cybersecurity. (D-1 nonexpert)

	There's a lot of debate out there about boards having a designated cyber expert. I'm in the camp of, it depends. It depends on what kind of company it is. But definitely, the board has to have enough knowledge to understand risk presented by cyber risk, and then have confidence that management is executing to mitigate that risk. (E-6) I think when you look at the board and the function of the board, you really want people that are very broad based in knowledge. And not necessarily deep expertise. The most important role of the board is that financial fiduciary responsibility. Certainly, you're going to have accounting and audit practitioners and things like that.... [W]hen you give a board seat that's dedicated to technology, or cyber, or some combination [thereof]..., is that really benefiting the entire company? And for a technology company, it's probably yes. Certainly, in fact, most board members of a technology company ought to be somewhere out of the technology sphere. But we're not a technology company, although we're obviously more and more dependent on technology. (E-6) I'm not opposed to [having a cybersecurity expert on the board], but I think that the board having the ability to directly contract for ancillary support is probably a shorter-term solution. I think in a long-term solution, I think that's a great idea. But again, I wouldn't just put a cybersecurity person in there. I would put somebody in there who understands the holistic environment of security and risk. (C-5) And so I see this debate a lot about do we need a cyber expert, and my personal opinion on that is many of us have dealt with cyber in managing our own companies, and people like [Director X] who've had a variety of military experience and the like, but to get someone who was maybe a former CISO, they may not make the best board member because they don't have the broader experience. And, in fact, I think we should be relying on the company hiring great expertise to manage the risk and us being at more of the oversight role. But, having said that, I think, again, that's why it's so high on the list of risk is because just the nature of the subject matter is one that, even if you were an expert five years ago, you might not be so expert today. It's a tough area to manage. (D-16)
No	The shareholders do not expect their board members to be experts in cybersecurity. They expect the company to have experts in cybersecurity and to be effectively deploying those to manage the risks, and I think the boards rely on third parties much like we do in an audit. (D-4 nonexpert) I think that for the level of oversight that they're providing, that just to have a general understanding of awareness is important. I'm not necessarily sure if they have to have a deep level. (E-3)

Table C3 Additional Interview Evidence of What Qualifies as Expertise

What qualifies as relevant expertise
I think the cyber and the IT coming together is really what is what you need… I think if you have made it to the ranks of being a Fortune 500 CIO, you understand you're accountable for both. You're maybe in a smaller company that doesn't get that, then that can be a little bit different. But I think the pedigree of the CIO that's going to join a publicly traded company board is probably very much understanding [of both IT and cybersecurity]. (D-5 expert) [T]here are luminary CISOs out there who understand how to make the connection between business and cybersecurity, who retire and join boards, and those are the ideal people. But… because you've got limited spots [on the board] from a governance perspective, to have somebody who's a single-threaded cybersecurity expert, you've got to be a heavy technology or [intellectual property]-based company to make that investment in the person, period. (C-7) I think they have had to physically run [the cybersecurity] organization at scale in some company or have run an oversight organization. Maybe they came out of the US government, and they are in the private sector now, or they're in the private sector now where they've come from some public organization, and they have that responsibility. (E-8)