Management Science

Publication details, including instructions for authors and subscription information:
http://pubsonline.informs.org

Inexpert Supervision: Field Evidence on Boards' Oversight of Cybersecurity

Michelle R. Lowry, Anthony Vance, Marshall D. Vance

To cite this article:
Michelle R. Lowry, Anthony Vance, Marshall D. Vance (2026) Inexpert Supervision: Field Evidence on Boards' Oversight of Cybersecurity. Management Science 72(2):783-804. https://doi.org/10.1287/mnsc.2023.04147

https://pubsonline.informs.org/journal/mnsc

MANAGEMENT SCIENCE
Vol. 72, No. 2, February 2026, pp. 783–804
ISSN 0025-1909 (print), ISSN 1526-5501 (online)

Inexpert Supervision: Field Evidence on Boards' Oversight of Cybersecurity

Michelle R. Lowry,[a] Anthony Vance,[b] Marshall D. Vance[a,*]

[a] Accounting and Information Systems Department, Pamplin College of Business, Virginia Tech, Blacksburg, Virginia 24060; [b] Department of Business Information Technology, Pamplin College of Business, Virginia Tech, Blacksburg, Virginia 24060

*Corresponding author

Contact: michellel@vt.edu, https://orcid.org/0000-0002-0701-7425 (MRL); anthony@vance.name, https://orcid.org/0000-0002-4554-6176 (AV); mdvance@vt.edu, https://orcid.org/0000-0002-4636-1691 (MDV)

Received: December 19, 2023
Revised: July 26, 2024; October 9, 2024
Accepted: October 25, 2024
Published Online in Articles in Advance: May 23, 2025

https://doi.org/10.1287/mnsc.2023.04147

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 diligent oversight, without expertise their efforts lack substance and therefore are mostly symbolic, even when they perform the same oversight activities as expert directors. We also explore why boards do not prioritize the appointment of 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 merits of board-level cybersecurity expertise.

History: Accepted by Ranjani Krishnan, accounting.

Funding: This work was supported by a Security, Privacy, & Trust grant from the Pamplin College of Business and the Commonwealth Cyber Initiative of Virginia.

Supplemental Material: The online appendix is available at https://doi.org/10.1287/mnsc.2023.04147.

Keywords: corporate governance • boards of directors • board oversight • risk oversight • cybersecurity risk • agency theory • institutional theory • expertise • qualitative field study

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 U.S. Securities and Exchange Commission (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% 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% 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 oversight" (New York State Department of Financial Services 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, whereas institutional theory argues that boards are motivated to adopt legitimate oversight behaviors that may take on a ceremonial character. However, prior research provides evidence that neither theory fully explains oversight practices and that boards display a mix of both substantive and symbolic oversight (Kalbers and Fogarty 1998, Beasley et al. 2009, Cohen et al. 2010, Clune et al. 2014, Trotman and Trotman 2015, Couchoux 2024). 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 the 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 that 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 functionally symbolic, even if not intentionally so. 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.

Research Question. *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 gain in-depth insights into boards' monitoring activities and decision-making (Yin 2018), which have been used in recent accounting research (Bills et al. 2018, Hayne and Vance 2019, Dodgson et al. 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 suggests that cybersecurity expertise is an important factor in influencing 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; thus, directors seek guidance on legitimate oversight practices from regulators, industry groups, and peer firms. However, we conclude that, in many cases, these oversight practices may 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. Most of our expert 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). Furthermore, inconsistent with independent monitoring under agency theory, we find that a lack of cybersecurity expertise leads some boards to heavily rely 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] Our interviews suggest that without expertise, directors are less likely to perceive CISOs giving self-serving reports (e.g., by filtering or obfuscating information) to be a barrier to cyber risk assessment and oversight, whereas expert directors, consultants, and even CISOs widely believe this to be an important issue. In addition, inexpert directors are less able to detect when CISOs filter reports, 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 important for substantive oversight—we also explore the reasons why relatively few boards have appointed cybersecurity experts. Most of our interviewees emphasized practical constraints, such as the scarcity of expertise in the director labor market and the emergence of cybersecurity as a top risk. However, our analysis suggests another fundamental reason for boards not appointing cybersecurity experts: nonexpert directors believe that they can provide adequate oversight despite not having cybersecurity expertise because of their general business and oversight experience, coupled with following best practices that they perceive to be legitimate. In contrast, expert directors perceive improvements in oversight effectiveness when boards have genuine cybersecurity expertise, and this view is also shared by CISOs and consultants. Overall, we conclude that when boards have cybersecurity

expertise, they are more likely to provide substantive oversight, as expected under agency theory. Although boards generally seek out best practices, consistent with institutional theory, when there is a lack of expertise, these practices are more likely to be motivated by legitimacy concerns and lack effectiveness and thus constitute primarily ceremonial oversight. This is the case even when nonexpert directors conduct oversight activities similar to those of expert directors.

We answer research calls to better understand the "differences in the form and substance of corporate governance" (Cohen et al. 2008b, 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 may increase the board's uncertainty regarding both underlying cybersecurity risk and related oversight tasks such that boards tend toward isomorphism by adopting legitimate but largely 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 et al. 2008b, p. 194, emphasis added). We enrich this theory by finding that nonexpert directors perform ritualistic activities because they *themselves* believe that these activities are legitimate and effective. Furthermore, 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 other C-level executives (Lowry et al. 2022); hence, we find that low expertise is a novel reason board members rely more heavily on and defer to management.

We also contribute to the debate on the need for cybersecurity expertise on boards (Larcker et al. 2017, Ferracone 2019). Our findings provide useful insights for regulators' and market participants' board composition decisions relative to cybersecurity expertise. Cybersecurity risk governance and disclosure continue to be high priorities for SEC rulemaking (SEC 2021a, b, c, d, 2022, 2023). Furthermore, in its proposed rule, the SEC asserts that directors' cybersecurity expertise is relevant to investors (SEC 2022). Although the importance of board financial expertise is well established in the literature, the SEC's proposal to require cybersecurity expertise disclosures similar to those for financial expertise was met with controversy[4] and was later removed in its final rule (SEC 2023). Moreover, most public company boards do not have a cybersecurity expert, suggesting that the need for expertise in this domain remains an open question. Although addressing the optimal level of board cybersecurity expertise is outside the scope of our analysis, our field evidence suggests that in the absence of expertise, boards may be more likely to provide symbolic oversight and may rely 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 increase the 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 (McDaniel et al. 2002, Agrawal and Chadha 2005, Fich and Shivdasani 2007, Cohen et al. 2014, Baugh et al. 2022). Although 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 that 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 who are agreeable to monitoring but do not explore whether differences in oversight behaviors extend beyond this selection effect. Similarly, Cohen et al. (2010) discuss audit committee (AC) members' financial expertise and power interchangeably, suggesting that expertise confers power; however, they do not directly assess how expertise affects oversight behaviors. We extend this line of research by providing evidence on how expertise affects a range of oversight activities.

Moreover, our examination of the role of expertise in the context of an emerging board responsibility where expertise is scarce is important given that prior research has focused on financial reporting oversight, for which expertise is common (Beasley et al. 2009, Cohen et al. 2010, Couchoux 2024). For instance, Couchoux (2024) finds that AC members self-select complementary roles based on their relative financial expertise. However, in contrast to Couchoux's setting, in which all ACs have at least one financial expert and all AC members are financially literate, board cybersecurity expertise is the exception rather than the rule. Thus, the "different combinations of styles" *within* an AC theorized by Couchoux (p. 484) are generally not applicable given the low expertise in the cybersecurity oversight setting. We answer the call of Couchoux (2024) for "more investigation into the differences between expectations for governance practices and actual practices" (p. 485). Given the increasing expectations for boards to oversee cybersecurity risk (e.g., as illustrated by the SEC's repeated emphasis on the board's role in this area), research on this emerging board responsibility is particularly needed. Since specific responsibility for cybersecurity oversight is often placed on ACs (Center for Audit Quality and Deloitte 2022) and financial experts

are rarely also cybersecurity experts, our findings provide timely feedback to ACs on one of their key responsibilities.

2. Background and Related Theory

2.1. Background

Cybersecurity incidents are increasingly common, costing billions of dollars annually in the United States alone (Federal Bureau of Investigation 2024). These incidents cause operational disruptions, reputational costs, worse loan terms, and loss of market value (Huang and Wang 2021, Kamiya et al. 2021, Tidy 2021, Tunggal 2021). In response, firms now spend more than $200 billion annually on cybersecurity, a figure projected grow at double-digit rates (Gartner 2023). However, experts believe that much of this spending is misdirected, underscoring the need for board-level oversight to ensure investments benefit shareholders (Morgan 2019, Internet Security Alliance, National Association of Corporate Directors 2020).

Reflecting these trends and concerns, there have been numerous calls for board-level oversight of cybersecurity risks. The Council of Institutional Investors states that "[e]ffective cybersecurity risk management starts with the board" (Council of Institutional Investors 2016, p. 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 specifically mandate such oversight. 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) (U.S. Department of the Treasury 2001).[5] The NYDFS and other state regulators issued similar rules for financial services firms (s 500.4[b]; NYDFS 2017, Blosfield 2021), and other industries are likely to adopt similar rules (PwC 2021). The NYDFS also updated its rules in 2023, requiring 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, cybersecurity oversight has been a focus 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 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 cybersecurity oversight and whether they receive direct reports from the CISO (SEC 2023).

Despite the urgency of effective cybersecurity programs and the expectations for directors to oversee them, surveys indicate that directors lack sufficient expertise to provide adequate oversight (National Association of Corporate Directors 2018). A survey of 577 U.S. public company directors finds that cybersecurity ranked *lowest* in perceived board effectiveness among the 19 responsibility areas considered, which the authors attribute to limited board-level experience or expertise (Cheng et al. 2021). This may be because ACs, traditionally focused on financial reporting, often oversee cybersecurity risk (Center for Audit Quality and Deloitte 2022).

2.2. Theoretical Lenses

We follow the suggestions of Malsch and Salterio (2016) for the use of theory in positivist field research. First, we consider the expectations and standards of investors and regulators 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 (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 literature (Beasley et al. 2009), particularly as it relates to boards' monitoring (as opposed to advising) role. Therefore, we use an agency perspective as a starting point from which to develop expectations for how boards respond to their emerging cybersecurity oversight responsibilities. We also incorporate perspectives from institutional theory to generate potential alternative predictions.[6]

Prior studies show that boards exhibit a range of oversight postures, from substantive to symbolic. Some studies have suggested that the 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). Although expertise has been cited as a potential differentiator, it has been conflated with director–management power dynamics (Cohen et al. 2010). In addition, although ACs largely exhibit substantive oversight over financial reporting (Beasley et al. 2009, Cohen et al. 2010), there is evidence that they exhibit more symbolic oversight over their other duties, such as enterprise risk management (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 because of 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, p. 323). Because of 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, p. 294). Hence, agency theory predicts that directors will be diligent monitors of material firm risks and executives over those risks, including cybersecurity risk.

The agency perspective of corporate governance broadly assumes that the board possesses general monitoring expertise that enables it to provide an independent[7] check on management (Fama and Jensen 1983). However, domain-specific expertise is increasingly recognized as important for boards to fulfill their intended monitoring role (Hillman and Dalziel 2003, Hambrick et al. 2015). Although there is limited existing 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 AC (DeFond et al. 2005).[8] As with financial reporting, cybersecurity is a technical domain; thus, boards' oversight of their firms' cybersecurity programs may similarly benefit from 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 because its predictions for board oversight have been contrasted with those of agency theory (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 that the board's goal is to achieve legitimacy in its oversight practices. However, an emphasis on perceived appropriateness can lead to symbolic rather than substantive oversight (Cohen et al. 2010, Bromley and Powell 2012, Wijen 2014).

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 mimic the governance behaviors of "leading" organizations for the sake of legitimacy (Cohen et al. 2008a), which may or may not result in effective oversight. Early interpretations of symbolic action under institutional pressures were framed as a decoupling of policy and practice (symbolic adoption). However, 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 but still not substantively improve oversight. For example, board questioning of executives may be the appropriate means (i.e., a legitimate oversight behavior), but if questioning is superficial, it will likely not result in the desired end (i.e., substantive oversight). Furthermore, this decoupling may occur due to domain uncertainty rather than being driven by self-interest (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 are likely to be especially prevalent in our setting.

Furthermore, 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 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 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 take actions that appear legitimate but may largely be only symbolic. To the extent that a lack of domain expertise increases uncertainty, we expect nonexpert boards to adopt practices that appear legitimate but may lack effectiveness due to low 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).[9] Thus, qualitative methods are required to open the "black box" of boards' governance of cybersecurity to better 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 (Malsch and Salterio 2016, Bills et al. 2018, Hayne and Vance 2019, Dodgson et al. 2020, Free et al. 2021).

To explore possible themes, theories, and issues relevant to cybersecurity oversight, we reviewed SEC and Public Company Accounting Oversight Board reports and guidance on cybersecurity oversight, regulatory cybersecurity roundtables, and guidance from practitioners and academics (Institute of Internal Auditors 2010, SEC 2011, Public Company Accounting Oversight Board 2018, SEC 2018, National Association of Corporate Directors 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 prepare an initial interview script (Yin 2018).[10]

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 an interviewee group that was diverse across a number of dimensions, as summarized in Table 1.[11] Panel A shows that among the 20 directors, 5 had cybersecurity expertise, which we categorized based on the 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 in the AC 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.[12] 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 the oversight provided, we also interviewed cybersecurity experts—executives (11 participants) and senior-level consultants (7 participants)—who support boards of directors.[13] 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, Miles et al. 2020, Ody-Brasier and Vermeulen 2020, Brühne and Schanz 2022). It is especially useful to substantiate observations from corporate "elites" (such as directors) with nonelites in organizational settings to avoid "provid[ing] only the 'top' part of a top-down perspective" (Odendahl and Shaw 2002, p. 314).[14] For three of our director participants, we were also able to interview a CISO who reports to them. In these cases, we could directly compare the perspectives of both parties in the oversight dyad.

Panel B of Table 1 presents information regarding the executive participants. Although the participants' executive titles varied, all the 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.[15] We continued our snowball sampling process until novel insights were no longer obtained (i.e., we reached theoretical saturation; Morse 1995, Malsch and Salterio 2016)—both for our director participants and for our cybersecurity experts.[16]

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

Table 1. Interview Details

Panel A: Director interview details

Interview no.	Interview length (min)	Committee participation related to cybersecurity	No. of positions	Years of director experience	Years at current largest firm	Cyber expertise	Experience in technical executive position (yr)	Market cap	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	Exec. director/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 no.	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 no.	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

Table 1. (Continued)

Panel C: Consultant interview details				
Interview no.	Interview length (min)	Position	Years of consulting experience	Type of 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

Notes. 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 work histories. With the exception of D-9 and D-18, who were executive directors, all the directors were independent directors. Market capitalization ranges are as follows: midcap, $2–9.9 billion; large-cap, $10+ billion, which is based on the director's largest firm, if publicly listed, or value upon privatization or annual revenues, if a private firm (P-private firm).

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 the participants preferred not to be recorded, a researcher or 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 online biographies. For those interviews with directors and cybersecurity executives, we also reviewed news articles, proxy statements, and annual reports related to the interviewees' firms. We followed a semistructured approach, customizing each interview script to the interviewee's position and background (see sample interview questions in the Online Appendix).

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. Overarching Themes of Boards' Oversight of Cybersecurity

An overarching theme of our findings is that cybersecurity has emerged as a top enterprise risk directors face, with the potential for companies across all industries (including traditional brick-and-mortar firms) to be taken offline because of a cybersecurity incident. Half of our director participants, particularly nonexperts, expressed concern and even anxiety about a company they oversee experiencing the next high-profile breach (such as Equifax or Colonial Pipeline). Accordingly, nearly half of the director participants volunteered that cybersecurity merits oversight by the entire board and 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 most[17] nonexpert director participants also stated that

boards generally lack expertise in cybersecurity compared with other domains, which poses challenges for boards for effective oversight. Although archival data (as noted above) suggest that board-level cyber expertise is uncommon, our participants shared mixed views regarding whether boards actively seek expert directors, a theme revisited at the end of this section.

Another overarching theme participants widely identified is that nascent norms and the evolving cyber landscape are unique challenges for substantive cybersecurity oversight over cybersecurity, particularly given boards' general lack of expertise. Most directors emphasized that best practices for cybersecurity oversight are still developing, and boards are struggling to understand their new responsibilities. Institutional theory predicts that boards 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 deemed "legitimate." Our data offer many examples of these isomorphic pressures shaping the way boards oversee cybersecurity.

A third overarching theme is that uncertainty tends to be greater when boards lack cybersecurity expertise. Illustrating how isomorphic pressures can shape oversight behaviors, a nonexpert director described looking to professional groups such as the NACD for guidance: "[I get guidance from] wherever I can … [the NACD has] a tremendous education program, lots of great meetings. … but candidly, *I'll take that and more*." (D-17, emphasis added). An important issue is whether nonexpert board members can effectively oversee cybersecurity by adopting such best practices; if not, these behaviors are more likely to be symbolic. In the following sections, we examine how expertise may influence the degree to which boards provide substantive or symbolic oversight, particularly in their engagement with cybersecurity oversight, questioning, relationship with management, and ability to detect false or withheld information on the part of cybersecurity management.

4.2. Effect of Expertise on Board Cybersecurity Oversight

4.2.1. Board Engagement with Cybersecurity Risk. In our sample, the boards received the CISO's report annually, quarterly, or in some cases, bimonthly—which can be seen as an indication of boards' attention to cybersecurity. Although at the time of our interviews, most boards were not required by law to receive these reports from management, we found that regular reporting by the CISO was nonetheless a best practice. This is unusual compared with 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, most expert and nonexpert directors expressed that they exercise diligence regarding 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, most directors (both expert and nonexpert) observed that boards' engagement with cybersecurity is moderated by directors' level of expertise. Several director participants indicated that they were brought onto boards for their particular expertise and would be 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). In such cases, although the board receives a report from cybersecurity management, directors may only passively listen.

Although past research suggests that directors with low expertise engage less in oversight of the related domain (Beasley et al. 2009, Couchoux 2024), the domain of cybersecurity oversight is noteworthy in at least two ways. First, some of our participants shared a perception that for many nonexpert directors, oversight of cybersecurity is largely motivated by and limited to compliance concerns and/or implementing best practices, potentially at the expense of seeking to understand and address a firm's specific cybersecurity risks. Thus, boards may adopt practices that are not suited to the firm's unique circumstances, or the practices may not be implemented effectively. Several of our participants shared that, although nonexpert board members recognize that cybersecurity is an increasingly important enterprise risk, some 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, some participants indicated that 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 and piqued by cybersecurity incidents. Several CISOs described receiving more questions about cybersecurity after prominent reports of breaches in the business press. These external cyber incidents serve as a "wake-up call" in which board members are prompted to ask, "Do we have the same risk?" (D-3 nonexpert). A concern raised about this reactive 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, some participants shared that this type of engagement may wane as a security incident becomes less salient in nonexpert directors' minds. By contrast, several expert participants, including an executive, mentioned that engagement with cybersecurity remains relatively constant for directors with high expertise.[18]

A powerful example of how directors' expertise can influence whether their engagement with cybersecurity is substantive is when directors voluntarily make efforts beyond formal oversight processes, which we term "stepping up." Participants described this type of oversight 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 the 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 can be even more demanding 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 [Chief Information Officer] 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 bimonthly 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, although stepping-up efforts from nonexpert directors can provide them with beneficial training and plausibly lead to *future* substantive oversight, this time is not spent on oversight. Instead, these training sessions increase the burden on executives without concurrently improving security programs.

Overall, our findings suggest that the level and effectiveness of board engagement, as expected by agency theory, hinge on the directors' expertise. As one expert director noted, "[B]oard members want to be useful. They want to make the company successful, and therefore, they are inclined to speak more about [their areas of expertise] and dwell on things where they feel like they can contribute" (D-9). Directors with low cyber expertise instead "lean into" areas they know well (D-7 nonexpert) and tend to direct their limited cybersecurity oversight on adopting practices they see as legitimate (as emphasized by institutional theory), which can effectively result in superficial oversight, as we further illustrate below.

4.2.2. Questioning. Our interviews revealed that questioning is a primary form of board oversight of cybersecurity, which is consistent with prior board literature in other domains (Gendron and Bédard 2006, Beasley et al. 2009, Kang et al. 2015). Some 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 information. … 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, several directors and executives 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 participants shared that nonexpert directors are more likely to ask fewer, basic, or perfunctory questions. Table 2 presents a summary of the contrasting opinions on the effect of expertise on questioning by participant expertise.[19]

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. Some expert participants described nonexpert directors asking questions to improve their general understanding of cybersecurity and related risks (e.g., what the risks are 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 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, an expert director described the tendency of nonexpert directors to depend on lists disseminated by professional groups (e.g., NACD) for questions that directors "should" ask without fully grasping them (D-13). Third, several 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)

Similarly, a consultant shared, "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). These examples illustrate how, in the absence of expertise, normative isomorphism can contribute to symbolic oversight. That is, although nonexpert directors may ask questions drawn from respected sources (i.e., questions that are perceived as legitimate), their lack of expertise may result in questioning that is more superficial in terms of the oversight provided.

In contrast to the questioning of nonexpert directors, 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 level 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.[20] Finally, just as expertise enables directors to ask more incisive questions, expertise similarly allows directors to better understand the answers they receive from executives. Furthermore, some interviewees described expertise as particularly important for enabling a director to ask valuable follow-up questions. A consultant explained this as follows:

> *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 branching logic, based on how the CISO is providing his or her updates.* (C-6)

Our participants perceived expertise as leading to substantive questioning and dialogue, aligning with agency theory. Our evidence suggests that both expert and nonexpert directors seek to oversee cybersecurity by asking questions of the CISO. In this way, nonexpert directors exhibit legitimate behaviors. However, participants suggest that because effective questioning depends on expertise, nonexpert directors' efforts may lack substance, and therefore primarily result in a symbolic oversight exercise.

4.2.3. Relationship with Cybersecurity Management.

Both the expert and nonexpert directors we spoke with generally emphasized the importance of working together with management to determine the best way to manage

Table 2. 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	Percentage	*N*	Percentage	*N*	Percentage
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

Is director questioning substantially affected by expertise–Yes

[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)

Is director questioning substantially affected by expertise–No

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)

Notes. This table presents participant views on the role of expertise in director questioning by participant type. Panel A presents a summary of participants' views on whether director questioning is substantially affected by cybersecurity expertise. Each participant's view was coded by two authors, and any disagreements were reconciled. Panel B presents representative quotes underlying this coding.

cybersecurity risk. The fact 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 appeared to be more willing to rely on CISOs to an unusual degree due to their lack of familiarity with this growing and evolving subject matter. Expert participants described this sort of support of the board as "coaching" (D-9 expert, C-5, C-6), a term we use to label a range of activities in which boards heavily rely on the CISO. Participants shared examples of coaching behaviors, including 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, most of our participants indicated that when board members have limited cybersecurity experience, educating the board was viewed as an important part of the CISO's responsibilities.[21] 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). Nearly all of our CISO participants described efforts to educate, or "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 noted 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 and why they would be needed. But if you say, "I need a new piece of software to do data loss prevention … ," now you may need to explain what that means, why they should care, and what the consequences are."* (C-1)

When directors have low cybersecurity expertise, they may use their already constrained attention to educate themselves rather than on substantive oversight, as highlighted by one expert director: "The audit committee [who typically are not cyber experts] will suck up 90% of the time worrying about the numbers and 10%, if

they're lucky, trying to understand cybersecurity, which they never will" (D-12 expert).

In addition to receiving training from CISOs, nonexpert directors often rely on CISOs to set expectations for how a security program should function and what the appropriate levels of risk might be. For example, a 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 cybersecurity maturity would be appropriate for the firm to target (a highly strategic decision) and a CISO negotiating with the board to establish realistic expectations about the inevitability of breaches.

Some expert participants shared that nonexpert directors often do not know what aspects of the cybersecurity program they should review to provide oversight. In these cases, CISOs not only set expectations but also play a key role in determining what is reported to the board. One CISO explained, "[T]he boards really don't know what they want to know.... 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 striking example of circular governance, a CISO provided the board with a list of questions they should ask him or her.

In contrast to the relationship that nonexpert directors have with CISOs, we find that expert directors generally do not require education from management because they already have an understanding and awareness of cybersecurity threats. Similarly, directors with high expertise often do not need expectations to be set for them because they already "know what good looks like" (D-5 expert, C-6) and what information they want reported to them. Thus, rather than relying on "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 the following:

> *[Having a cybersecurity expert on board] really calls and exacts more of the CISO who is going into the [boardroom], 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 depend on the CISO for coaching.

Although boards receiving reports directly from the CISO is a best practice and is required in some industries (e.g., the 2023 FTC Safeguards Rule for financial institutions), the analysis above illustrates that it may not result in substantial oversight if a board has low cybersecurity expertise. In these cases, uncertainty surrounding cybersecurity may lead boards with low expertise to effectively cede 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, such as setting benchmarks and the scope of relevant cybersecurity risks. Overall, this dynamic is not consistent with the expectations of agency theory that boards provide independent oversight. Instead, our findings suggest that boards with low expertise perform legitimate actions (e.g., receiving reports from CISOs) that may ultimately lead to more symbolic oversight.

4.2.4. Detecting False or Withheld Information in Management Reports.

A particularly stark manifestation of the agency conflict between the board and CISO is the observation that some CISOs filter cybersecurity reports to improve their boards' assessment of cybersecurity performance. Generally, these efforts are described by participants as CISOs sometimes overstating their performance or understating cybersecurity risks to make themselves (or often, their boss such as the CIO) look better. For example, a consultant characterized this as avoiding "telling (the board) all of your Achilles' heels and all the things you screwed up on" (C-4). A CISO acknowledged that "the truth hurts sometimes," and cited conversations with colleagues at other companies who are not "willing to state the facts and try to paint a prettier picture" or who felt a need to "craft the message" to "make themselves look good" (E-1). Describing these sorts of filtering efforts, a consultant shared, "I have seen very talented CISOs outmaneuver, outtalk, outconvince boards. … They would just use their likability and personality to put the board at ease when things weren't going well." (C-6)

The most frequently shared consequence of filtering is that the board is not able to make an accurate assessment of the company's cybersecurity risk or the effectiveness of management's efforts to address these risks. Therefore, CISO filtering may present a barrier to boards' ability to perform their risk oversight responsibilities. Management obfuscating information is not isolated to the cybersecurity setting (nor are the underlying agency conflicts, as discussed in Section 2.3), 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 may be particularly high in the cybersecurity setting due to the technical evolving nature of the risk and a general lack of cybersecurity expertise among directors.

Because of the sensitive nature of this issue, we asked participants whether it was common for CISOs at other companies to filter their reports. When asked about the potential for filtering, most nonexpert directors expressed the belief 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, the majority of executives and consultants we interviewed believe that some CISOs obfuscate their reports to boards to make themselves or other executives look better. For instance, a CISO candidly shared their 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)*

Furthermore, this CISO shared that the new CIO "refused" to show the board performance measures that reflected poorly on the efficiency of cyber investments because the CIO wanted to demonstrate improvement to the board.

To corroborate our expert interviewees' views that opportunistically filtering reports is a common practice, we surveyed an additional 33 CISOs.[22] 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 median is 40% of CISOs, and all but one respondent reported a nonzero percentage.[23]

Similarly, expert directors tended to be more aligned with our CISO and consultant participants on this issue because all but one acknowledged the potential for CISO obfuscation (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). When asked whether CISOs might be able to successfully filter or provide false information to the board because most board members have low knowledge of cybersecurity, another expert director 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, our findings indicate that CISOs opportunistically filtering reports to boards potentially limits the effectiveness of board oversight, although nonexpert directors downplay this concern.

In addition to being aware of the risk of CISO filtering, cybersecurity expertise also enables directors to

Table 3. Perceptions of CISO Filtering

Panel A: Summary of views by participant category

	Nonexpert		Director experts		Executive/consultant experts	
Is CISO filtering a concern?	*N*	Percentage	*N*	Percentage	*N*	Percentage
Yes	4	38.5%	4	80.0%	12	75.0%
No	7	46.2%	0	0.0%	4	25.0%
Mixed	1	15.4%	1	20.0%	0	0.0%

Panel B: Representative quotes

Is CISO filtering a concern–Yes

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)

Is CISO filtering a concern–No

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)

Notes. This table presents participant views on CISO filtering by participant type. Panel A presents a summary of participants' views on whether CISO filtering was a concern in cybersecurity risk oversight. Each participant's view was coded by two authors, and any disagreements were reconciled. Panel B presents representative quotes underlying this coding.

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). Some participants shared that expert directors can challenge CISOs who skirt around root issues or report diversionary or incomplete information. One expert director explained that with expertise, directors "want to see real 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 appears to influence directors' perceptions of the risk of CISO filtering and their ability to detect it. Our finding that many directors may not fully recognize the potential for incentive conflicts is inconsistent with expectations from agency theory. Rather, nonexpert directors who ceremonially receive reports (a legitimate practice) may be less likely to recognize managers' incentives or ability to obfuscate information are more consistent with the means of oversight being decoupled from the desired ends, as suggested by institutional theory.

4.2.5. Summary of the Effects of Expertise on Board Cybersecurity Oversight. The findings of Section 4.2 underscore the assumption of agency theory that directors have sufficient expertise to provide substantive independent oversight (Fama and Jensen 1983, Jensen 1993). Our findings suggest that although both expert and nonexpert directors engage with cybersecurity oversight, our respondents perceived that questioning and monitoring of the CISO and cybersecurity program may be more substantive when directors have expertise. Without it, following best practices could result in less effective oversight, potentially serving more of a symbolic function. An example of how a lack of expertise can lead to a decoupled focus on legitimacy rather than effectiveness was given by a nonexpert director, who described their perceptions of boards spending on cybersecurity:

> *I don't think there's a limit on the amount of money that the marketplace would spend to somehow check the box that we did what we need to do to protect ourselves against cyber risk, even though oftentimes people don't really understand how much they're really mitigating that risk and that sort of thing … a lot of times investments are made without … a clear sight line as to whether those are really the right investments or what the value of those investments are … . (D-6 nonexpert)*

In summary, when directors lack cybersecurity expertise, there may be a decoupling of means (legitimate behaviors) and ends (substantive oversight), aligning with institutional theory.

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

Our director participants unanimously cited cybersecurity as one of the most critical enterprise risks for boards. However, our findings indicate that when boards lack expertise, 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 may lack substantive effects. As discussed previously, agency theory presumes boards have the expertise to provide effective oversight, yet survey evidence shows this 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 and find that only 14.7% of firms disclosed at least one director with cybersecurity or related skills and experiences, which is consistent with another contemporary analysis (Rundle 2023).[24] Thus, in the archival data, we observe that appointing directors with cybersecurity expertise may not be a high priority for most boards. A natural question then arises: If directors believe that cybersecurity is a critical enterprise risk, why do boards not seek the expertise needed to provide substantive oversight, as predicted by agency theory?

Our analysis suggests several potential explanations for why boards may not appoint cybersecurity experts. First, both expert and nonexpert participants described practical constraints. For example, some participants shared challenges in such hiring because of the scarcity of bona fide cybersecurity experts in the director labor market. A related reason is the common perception that directors with cybersecurity expertise may contribute little beyond cybersecurity and that companies should not "give up a board seat" for a cybersecurity expert who cannot contribute to other areas of the business (C-2). Some nonexpert directors expressed concern that such an appointment could lead to over-reliance on that person or a false sense of security. Additionally, one expert director pointed to the recent emergence of cybersecurity as critical enterprise risk as a reason for the lack of board-level expertise.

However, our analysis suggests that practical constraints may not fully explain the expertise gap. Large companies could likely attract directors with cyber expertise if they prioritized doing so, notwithstanding the shallow talent pool.[25] Likewise, board size is not necessarily constrained and could accommodate directors with cybersecurity expertise if deemed necessary. Finally, because the SEC has called for corporate cybersecurity disclosures since 2011 (with additional emphasis over time; SEC 2011, 2018, 2023), insufficient time alone does not seem to fully account for the lack of board-level expertise.

A second compelling reason why boards may not prioritize appointing cybersecurity experts is that many nonexpert directors believe that they can provide adequate cybersecurity oversight through their general experience, notwithstanding their lack of specific expertise. For example, some nonexpert directors expressed that their general business experience and abilities as board members adequately qualified them to oversee cybersecurity risk. This may partially stem from underestimating potential agency conflicts with the CISO, such as the CISO's incentive to filter reports to the board. Several nonexpert directors also shared that broad business experience is more valuable than deep expertise in cybersecurity because broad experience enables "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 view of some participants on appointing a director with cybersecurity expertise:

> *I see this debate a lot about, "Do we need a cyber expert?" … 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. … 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)*

Another 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 … have a better perspective on understanding business risk … in [a] holistic context [rather] than dropping you down into this technical silo" (D-6 nonexpert). These statements reflect directors' confidence in providing oversight by virtue of their general experience. As discussed above, nonexpert directors pointed to following emerging best practices, such as asking "the right questions" (D-3 nonexpert) and receiving reports and other regular interactions with CISOs as evidence of the legitimacy of their oversight. In addition, some nonexpert directors pointed to cybersecurity training through NACD or similar professional organizations as aiding their oversight. Nonexpert directors' executive experience at a digital or technology firm was cited by some participants as adjacent expertise that enables boards to provide adequate cybersecurity oversight. Finally, most nonexpert directors cited their ability to contract consultants to compensate for their boards' lack of cybersecurity expertise.

In contrast, our expert participants provided an alternative perspective, seeing directors' lack of expertise as a major impediment to effective oversight (see Table 4 for a summary of these contrasting opinions). For example, an expert director strongly challenged the idea that general expertise qualifies boards to oversee cybersecurity stating:

> *[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)

Several expert participants expressed skepticism that brief training sessions could provide the expertise needed for substantive cybersecurity oversight. Furthermore, some experts noted that technology expertise is not equivalent to cybersecurity expertise because "cyber is its own discipline" with "a different mindset and a different set of tools" (D-9 expert).[26] Several expert participants warned that relying on consultants for cybersecurity expertise can effectively result in an outsourcing of oversight and that nonexpert directors may struggle to determine what types of cybersecurity engagements are needed or to evaluate the quality of consultants' work. Finally, some expert participants pointed to the hollowness of following best practices when boards lack the expertise 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 value of board-level expertise. When asked whether having a board-level expert would improve oversight, the director responded, "I don't see how it would" (D-18 nonexpert); however, the CISO candidly shared a contrasting belief, claiming that an expert director would result in more structured and in-depth oversight.

In summary, although our study does not aim to determine the optimal level of board cybersecurity expertise, we provide contrasting opinions about and rationales for the need for cybersecurity experts on boards. While acknowledging that cybersecurity expertise is helpful, the majority of nonexpert directors shared that they do not believe that effective oversight requires domain expertise; they provided important practical reasons for not appointing experts, but more revealingly, they asserted that general business expertise, supplemented with third-party consulting, is sufficient for effective oversight. However, experts generally believe that substantive and independent assessment requires domain knowledge gained from hands-on experience.

5. Discussion and Conclusion

Our participants uniformly perceived cybersecurity risk oversight as being 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

Table 4. Is Expertise Needed?

Panel A: Summary of views by participant category

	Nonexpert		Director experts		Executive/consultant experts	
Is expertise needed for effective cybersecurity risk oversight?	*N*	Percentage	*N*	Percentage	*N*	Percentage
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 quotes

Is expertise needed for cybersecurity oversight–Yes

[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)

Is expertise needed for cybersecurity oversight–No

[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)

Notes. This table presents participants' views on the need for board-level cybersecurity expertise by participant type. Panel A presents a summary of participants' views on whether cybersecurity expertise is needed for effective cybersecurity risk oversight. Each participant's view was coded by two authors, and any disagreements were reconciled. Panel B presents representative quotes underlying this coding.

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 may be less likely to perceive a significant difference in effectiveness between expert and nonexpert directors because they believe their performance of legitimate best practices results in substantive oversight and, therefore, do not see the need to appoint directors with bona fide cybersecurity experience. In contrast, the expert directors, executives, and consultants we interviewed see a clear difference in oversight performed by experts versus nonexperts, arguing 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 fully explains boards' cybersecurity oversight. Instead, our analysis suggests that bona fide cybersecurity expertise is a key contingency for whether substantive or symbolic oversight is performed. In other words, expertise is a boundary condition for whether agency theory or institutional theory more accurately explains boards' oversight of cybersecurity. Specifically, we explore how expertise relates to the decoupling of means and ends in the context of the highly uncertain field of cybersecurity governance. Therefore, this study contributes an important theoretical contextualization of agency theory and institutional theory in the domain of cybersecurity oversight (Johns 2006, 2017).

Our study provides novel theoretical insights compared with prior research. First, Gendron and Bédard (2006) interviewed AC meeting participants in three large Canadian firms and find that AC members reflectively believe that they are effective because they have domain (i.e., financial) expertise. In contrast, our findings suggest that directors believe that 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 AC. In contrast, the executives and consultants we interviewed generally do not perceive such ceremonial features as particularly effective when expertise was lacking.

Third, several recent studies find that management can have an outsized influence on the terms of board oversight (Cohen et al. 2002, 2010; Beasley et al. 2009; Clune et al. 2014),[27] similar to the circular governance we observe. These papers often point to CEO power and board–CEO social ties as key factors leading directors to cede oversight control to management. In our setting, however, nonexpert directors rely heavily on management such that they 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" because they often struggle to achieve legitimacy within the executive suite (Lowry et al. 2022).[28] 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, our findings suggest that nonexpert board members respond to the uncertainty inherent in cybersecurity risk oversight by seeking out and performing best practices that they *themselves* believe are legitimate, even though experts may view these efforts as less effective. This suggests a potential blind spot in directors' self- and board-level evaluations, wherein there is a decoupling of means (legitimate oversight behaviors) and ends (substantive oversight), as predicted by institutional theory. 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) propose 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 limited effect on cybersecurity outcomes.

We answer calls for additional research to examine the role of ACs, especially those related to emerging oversight responsibilities (Hermanson et al. 2024, Cunningham et al. 2025). Importantly, our setting is characterized by a scarcity of domain expertise, which starkly contrasts with qualitative studies touching on the role of financial expertise in the AC. For example, all three ACs in the study of Gendron and Bédard (2006) are characterized as having an "extensive financial and accounting background" (p. 219). Similarly, Couchoux (2024) notes that financial literacy is a baseline requirement for AC members of public companies and finds that AC members' conceptualization of their degree of knowledge informs their financial reporting oversight styles.

Although our study shares similarities with Couchoux (2024), notably in examining the role of expertise in shaping oversight, our study differs in important ways. Couchoux (2024) adopts a social-constructivist lens to examine how *individual* AC members understand their roles based on their own perceptions of their level of financial reporting knowledge. As a result, Couchoux's analysis and implications are primarily at the individual-director level. This granular approach is warranted in the well-studied financial reporting oversight context, but the attendant individual reflective understandings of their style based on their knowledge does not directly extend to board-level effectiveness. In contrast, we use agency and institutional theory to form more outcome-oriented expectations, focusing on how individual directors' efforts contribute to *board*-level oversight effectiveness. This difference is reflected in our choice of participants, as we interview not only directors, but also the executives they oversee and the consultants who support them to provide a more holistic picture of board-level oversight. Although both studies find that low expertise leads to more symbolic oversight, the implications of our findings are very different. Couchoux (2024) finds that in financial reporting oversight, AC members choose complementary oversight styles that align with their relative financial expertise. This is useful for understanding board dynamics in settings like financial reporting, where experts may take on more stringent monitoring, whereas less expert directors may *individually* adopt a symbolic role, relying on the experts to do the heavy lifting. In contrast, an implication of our findings is that with cybersecurity (and possibly other emerging board responsibilities), boards *as a whole may* perform symbolic oversight. Moreover, Couchoux (2024) concludes that AC members' perceptions of their relative expertise shape "what they do to oversee financial reporting" (p. 462). In contrast, we find that nonexpert directors, while seeking legitimacy by mimicking what experts do, often believe their oversight is on par with that of experts. However, these efforts may lack substance due to limited expertise.

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). Although our participants unanimously perceived board-level cybersecurity expertise as helpful, our interviews revealed that experts and nonexperts often have differing views on whether cybersecurity expertise is a requirement for effective oversight. Our analysis suggests a greater risk for cybersecurity-related corporate governance failures when nonexpert boards cede control of oversight. However, we note that the policy implications of our findings are not immediately clear. For example, our study does not encompass a full examination of the relative benefits of cybersecurity expertise versus other director qualifications, which plausibly vary across firms and therefore cannot directly speak to the optimal level of board cybersecurity expertise. Thus, although 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 has limitations common to interview-based field studies. For example, participants may not have been fully candid. We attempted to mitigate this 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. For instance, expert directors emphasize the importance of expertise, whereas nonexpert directors view it as less critical. Nevertheless, our interviews provided a range of perceptions based on participants' experiences with multiple boards with varying levels of cybersecurity expertise.

Our study suggests several avenues for future research. We specifically focus on cybersecurity risk

oversight, and although 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, future research on cybersecurity can explore questions raised by this study. Archival research can examine the benefits (e.g., reduced breaches, better insurance terms) and potential costs (e.g., increased board meetings, opportunity cost of board composition) of adding a cybersecurity expert to the board. The expanded cybersecurity oversight disclosures required by the 2023 SEC rules provide additional opportunities to examine questions raised by our study, such as the relationship between board expertise and disclosed oversight practices, and how these oversight practices relate to cybersecurity outcomes. Additionally, future research could examine how cybersecurity outcomes, such as data breaches, affect board turnover and composition, which reflect attitudes about the need for cybersecurity expertise. Given investors' and regulators' ongoing emphasis on board oversight of cybersecurity, we encourage future research to extend our study in these directions.

Acknowledgments

The authors thank the board directors, cybersecurity executives, and consultants who agreed to participate in this research and Chris Barhorst, France Bélanger, Mary Ellen Carter, Christie Hayne, Eldar Maksymov, Jeff Pittman, Vern Richardson, Sarah Stein, Kimberly Walker, David Wood, and the workshop participants at Arizona State University, Baruch College, the Brigham Young University Accounting Research Symposium, the Corporate Governance and Executive Compensation Research Series, the International Conference on Information Systems Accounting and Information Systems pre-conference workshop, Miami University, the University of Jyväskylä, the University of South Florida, Georgetown University, the Virginia Accounting Research Conference, and Virginia Tech for comments.

Endnotes

[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), https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

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

[3] For brevity, we refer to senior executives responsible for cybersecurity as "CISOs." These are typically executives that are two or more layers from the CEO, often through the chief information officer (Sahin and Vance 2025).

[4] As an illustration of this controversy, an analysis of SEC comment letters finds that comments against the disclosure rule outnumber those in favor nearly two to one. Details of this analysis are available in the Online Appendix.

[5] Notably, the OCC specifically cites the failure of Capital One's board to provide effective cybersecurity oversight in levying an $80 million fine for Capital One's 2019 data breach (U.S. Department of the Treasury 2020).

[6] Some studies have used additional theories, like resource dependence and management hegemony, to investigate corporate governance (Cohen et al. 2008a, Clune et al. 2014). Boards of directors play both monitoring and advising roles (Faleye et al. 2011), with agency theory and resource dependence theory serving as primary lenses for each, respectively (Hillman and Dalziel 2003). While acknowledging directors' advising role, we focus on monitoring, consistent with the SEC's guidance emphasizing board's cybersecurity oversight responsibilities. We did not anticipate, nor did we see evidence of managerial hegemony playing a role in board cybersecurity oversight.

[7] Although the governance implications of director independence have been well studied, most research focuses on structural independence, which is typically measured by a director's employment relationship with the firm or preexisting ties to the executive team (Weisbach 1988, Beasley 1996, Klein 2002, Chen et al. 2015). More fundamentally, independence refers to a director's ability to independently assess the firm's risks, programs, and performance separate from management's assessments (Hambrick et al. 2015).

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

[9] Approval for the use of human subjects was granted by the institution at which the research took place.

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

[11] Two director participants and four executive participants represent private firms; some directors held both public and private positions. Surprisingly, we found no significant variation in cybersecurity governance between public and private firms. Participants with experience on both (D-4 nonexpert, D-5 expert, E-5), indicated that oversight is similar. One director noted that their private firm had the best cybersecurity posture (D-15 nonexpert).

[12] 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).

[13] Throughout Section 4, we identify which participant group our findings relate to. However, in cases where the finding applies across all participant groups, we simply refer to "participants" or "interviewees."

[14] Cohen et al. (2010) interviewed auditors for an outside perspective on boards' oversight of financial reporting, whereas Beasley et al. (2009) interviewed board members. Noting this difference in perspectives, Cohen et al. (2010) suggest a need for further research to explore differences in these perspectives. In the spirit of this call, our interview pool allowed us to compare perspectives of multiple parties involved in the cybersecurity risk oversight process.

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

[16] Our coding process overlapped with our sampling process (i.e., we coded interviews while continuing to recruit participants), which helped us identify theoretical saturation. For example, each researcher independently identified themes raised in the interview during coding, we then held post interview coauthor meetings where we compared resultant theme memos and evaluated whether additional interviews produced new themes or insights. As evidence of saturation, we ceased creating new codes after our first 27 interviews.

[17] In Section 4, we use the terms "some" or "several" to refer to at least two participants but less than half, "most" to indicate at least

half but not all, and "all" to specify all participants. We provide additional participant quotes in the Online Appendix.

[18] Although this observation by expert directors may reflect self-serving bias, this is unlikely to reflect bias coming from an executive.

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

[20] A CISO provided a contrasting view that expert directors may be inclined to get too involved with cybersecurity, which can increase the time demands on the cybersecurity team.

[21] Although CISOs sharing this view may reflect self-serving bias, this concern is mitigated because this perspective was also expressed by directors and consultants.

[22] 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%.

[23] 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 the behavior of respondents' peers is a common way of reducing social desirability bias (Fisher 1993).

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

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

[26] It is well known in the IT space that cybersecurity is its own domain and that it is often in conflict with the IT function (Anderson 2020). Therefore, IT expertise does not necessarily translate to cybersecurity risk expertise.

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

[28] A contemporary interview study finds that CISOs struggle as a lower tier executive within the executive suite but that they can gain legitimacy through regulatory guidance and access to and support from the board of directors (Lowry et al. 2022). Our study has similar participants, but our focus is on the role of expertise on board oversight of cybersecurity while theirs focuses on developing a model of CISO legitimacy given the challenges of the CISO role.

References

Abbott LJ, Parker S, Peters GF (2004) Audit committee characteristics and restatements. *Auditing* 23(1):69–87.

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

Agrawal A, Chadha S (2005) Corporate governance and accounting scandals. *J. Law Econom.* 48(2):371–406.

Aguilar LA (2014) Boards of directors, corporate governance and cyber-risks: Sharpening the focus. Speech, June 10. Cyber Risks and the Boardroom Conference (SEC, Washington, DC), https://www.sec.gov/newsroom/speeches-statements/2014-spch061014laa.

Anderson R (2020) *Security Engineering: A Guide to Building Dependable Distributed Systems*, 3rd ed. (John Wiley & Sons, Indianapolis, IN).

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

Baugh M, Hallman NJ, Kachelmeier SJ (2022) A matter of appearances: How does auditing expertise benefit audit committees when selecting auditors? *Contemporary Accounting Res.* 39(1):234–270.

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

Beasley MS, Carcello JV, Hermanson DR, Neal TL (2009) The audit committee oversight process. *Contemporary Accounting Res.* 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* 23(2):13–35.

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

Blosfield E (2021) Maine one of latest states to enact NAIC-inspired Insurance Data Security Act. Accessed August 12, 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. *Acad. Management Ann.* 6(1):483–530.

Brühne AI, Schanz D (2022) Defining and managing corporate tax risk: Perceptions of tax risk experts. *Contemporary Accounting Res.* 39(4):2861–2902.

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

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

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

Cheng JY-J, Groysberg B, Healy P, Vijayaraghavan R (2021) Directors' perceptions of board effectiveness and internal operations. *Management Sci.* 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 Res.* 31(3):748–786.

Cohen JR, Krishnamoorthy G, Wright AM (2002) Corporate governance and the audit process. *Contemporary Accounting Res.* 19(4):573–594.

Cohen JR, Krishnamoorthy G, Wright AM (2008a) Form versus substance: The implications for auditing practice and research of alternative perspectives on corporate governance. *Auditing* 27(2):181–198.

Cohen JR, Krishnamoorthy G, Wright AM (2008b) The corporate governance mosaic and financial reporting quality. *J. Accounting Literature* 23:87–152.

Cohen JR, Krishnamoorthy G, Wright AM (2010) Corporate governance in the post-Sarbanes-Oxley era: Auditors' experiences. *Contemporary Accounting Res.* 27(3):751–786.

Cohen JR, Krishnamoorthy G, Wright AM (2017) Enterprise risk management and the financial reporting process: The experiences of audit committee members, CFOs, and external auditors. *Contemporary Accounting Res.* 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. *Accounting Rev.* 89(1):243–273.

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

Council of Institutional Investors (2016) Prioritizing cybersecurity. Report, Council of Institutional Investors, Washington, DC.

Cunningham LM, Stein SE, Walker K, Wolfe K (2025) Redefining perceived boundaries: Insights into the audit committee's

evolving responsibilities. *Accounting Rev.*, ePub ahead of print March 19, https://doi.org/10.2308/TAR-2023-0474.

DeFond ML, Hann RN, Xuesong HU (2005) Does the market value financial expertise on audit committees of boards of directors? *J. Accounting Res.* 43(2):153–193.

DiMaggio PJ, Powell WW (1983) The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. *Amer. Sociol. Rev.* 48(2):147–160.

Dodgson MK, Agoglia CP, Bennett GB, Cohen JR (2020) Managing the auditor-client relationship through partner rotations: The experiences of audit firm partners. *Accounting Rev.* 95(2):89–111.

Duchin R, Matsusaka JG, Ozbas O (2010) When are outside directors effective? *J. Financial Econom.* 96(2):195–214.

Edmans A, Gosling T, Jenter D (2023) CEO compensation: Evidence from the field. *J. Financial Econom.* 150(3):103718.

Eisenhardt KM (1989) Agency theory: An assessment and review. *Acad. Management Rev.* 14(1):57–74.

Faleye O, Hoitash R, Hoitash U (2011) The costs of intense board monitoring. *J. Financial Econom.* 101(1):160–181.

Fama EF (1980) Agency problems and the theory of the firm. *J. Political Econom.* 88(2):288–307.

Fama EF, Jensen MC (1983) Separation of ownership and control. *J. Law Econom.* 26(2):301–325.

Federal Bureau of Investigation (2024) Internet Crime Report 2023. Report, FBI, Washington, DC.

Federal Trade Commission (2021) Corporate boards: Don't underestimate your role in data security oversight. Report, Federal Trade Commission, Washington, DC.

Ferracone (2019) Good governance: Do boards need cyber security experts? 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. *J. Financial Econom.* 86(2):306–336.

Fiolleau K, Hoang K, Pomeroy B (2019) Auditors' communications with audit committees: The influence of the audit committee's oversight approach. *Auditing J. Practice Theory* 38(2):125–150.

Fisher RJ (1993) Social desirability bias and the validity of indirect questioning. *J. Consumer Res.* 20(2):303–315.

Free C, Trotman AJ, Trotman KT (2021) How audit committee chairs address information-processing barriers. *Accounting Rev.* 96(1):147–169.

Gartner (2023) Gartner forecasts global security and risk management spending to grow 14% in 2024. Report, Gartner, Stamford, CT.

Gendron Y, Bédard J (2006) On the constitution of audit committee effectiveness. *Accounting Organ. Soc.* 31(3):211–239.

Goh BW (2009) Audit committees, boards of directors, and remediation of material weaknesses in internal control. *Contemporary Accounting Res.* 26(2):549–579.

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. *Acad. Management Rev.* 40(3):323–344.

Hayne C, Vance M (2019) Information intermediary or de facto standard setter? Field evidence on the indirect and direct influence of proxy advisors. *J. Accounting Res.* 57(4):969–1011.

Hermanson DR, Hurley PJ, Obermire KM (2024) Audit committee research: Where do we stand, and where do we go from here? *Auditing* 43(3):165–185.

Hermanson DR, Tompkins JG, Veliyath R, Ye Z (2012) The compensation committee process. *Contemporary Accounting Res.* 29(3):666–709.

Hillman AJ, Dalziel T (2003) Boards of directors and firm performance: Integrating agency and resource dependence perspectives. *Acad. Management Rev.* 28(3):383–396.

Hoitash U, Hoitash R, Bedard JC (2009) Corporate governance and internal control over financial reporting: A comparison of regulatory regimes. *Accounting Rev.* 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. *J. Bus. Ethics* 84(4):497–527.

Huang HH, Wang C (2021) Do banks price firms' data breaches? *Accounting Rev.* 96(3):261–286.

Hwang B-H, Kim S (2009) It pays to have friends. *J. Financial Econom.* 93(1):138–158.

Institute of Internal Auditors (2010) *Global Technology Audit Guide (GTAG(R)) 15 Information Security Guidance* (Institute of Internal Auditors, Altamonte Springers, FL).

Internet Security Alliance, National Association of Corporate Directors (2020) *Internet Security Alliance and National Association of Corporate Directors Release New Guide for Cyber-Risk Oversight* (Internet Security Alliance, Arlington, VA).

Jackson RJ (2018) Corporate governance: On the front lines of America's cyber war. Speech, March 15 (SEC, Washington, DC), https://www.sec.gov/newsroom/speeches-statements/speech-jackson-cybersecurity-2018-03-15.

Jensen MC (1993) The modern industrial revolution, exit, and the failure of internal control systems. *J. Finance* 48(3):831–880.

Jensen MC, Meckling WH (1976) Theory of the firm: Managerial behavior, agency costs and ownership structure. *J. Financial Econom.* 3(4):305–360.

Johns G (2006) The essential impact of context on organizational behavior. *Acad. Management Rev.* 31(2):386–408.

Johns G (2017) Reflections on the 2016 Decade Award: Incorporating context in organizational research. *Acad. Management Rev.* 42(4):577–595.

Kalbers LP, Fogarty TJ (1998) Organizational and economic explanations of audit committee oversight. *J. Managerial Issues* 10(2):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. *J. Financial Econom.* 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 Organ. Soc.* 46:59–76.

Klein A (2002) Audit committee, board of director characteristics, and earnings management. *J. Accounting Econom.* 33(3):375–400.

Krishnan J (2005) Audit committee quality and internal control: An empirical analysis. *Accounting Rev.* 80(2):649–675.

Krishnan J, Wen Y, Zhao W (2011) Legal expertise on corporate audit committees and financial reporting quality. *Accounting Rev.* 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*, 17–70.

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 Res.* 36(4):2521–2553.

Lowry MR, Sahin Z, Vance A (2022) Taking a seat at the table: The quest for CISO legitimacy. *ICIS 2022 Proc.* (Association of Information Systems (AIS), Atlanta), 14.

Malsch B, Salterio SE (2016) "Doing good field research": Assessing the quality of audit field research. *Auditing* 35(1):1–22.

Masulis RW, Mobbs S (2014) Independent director incentives: Where do talented directors spend their limited time and energy? *J. Financial Econom.* 111(2):406–429.

McDaniel L, Martin RD, Maines LA (2002) Evaluating financial reporting quality: The effects of financial expertise vs. financial literacy. *Accounting Rev.* 77(suppl 1):139–167.

Miles MB, Huberman AM, Saldaña J (2020) *Qualitative Data Analysis: A Methods Sourcebook*, 4th ed. (Sage Publications, Thousand Oaks, CA).

Milica L, Pearlson K (2023) Boards are having the wrong conversations about cybersecurity. *Harvard Bus. Rev. Insight Center Collect.* (May 2), https://hbr.org/2023/05/boards-are-having-the-wrong-conversations-about-cybersecurity.

Morgan S (2019) Global Cybersecurity spending predicted to exceed $1 trillion from 2017–2021. *Cybercrime Magazine* (June 10), https://cybersecurityventures.com/cybersecurity-market-report/.

Morse JM (1995) The significance of saturation. *Qual. Health Res.* 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.

Myers MD (2009) *Qualitative Research in Business & Management* (Sage Publications, Thousand Oaks, CA).

National Association of Corporate Directors (2020) Cyber-risk oversight 2020: Key principles and practical guidance for corporate boards. Report, National Association of Corporate Directors, Arlington, VA.

New York Department of Financial Services (2017) Cybersecurity requirements for financial services companies. Report, New York State Department of Financial Services, Albany, NY.

New York Department of Financial Services (2023) 23 NYCRR 500: Cybersecurity requirements for financial services companies. Report, New York State Department of Financial Services, Albany, NY.

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.

Ody-Brasier A, Vermeulen F (2020) Who is punished most for challenging the status quo? *Acad. Management J.* 63(5):1621–1651.

Paternoster R, Simpson S (1996) Sanction threats and appeals to morality: Testing a rational choice model of corporate crime. *Law Soc. Rev.* 30(3):549–583.

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.

Public Company Accounting Oversight Board (2018) Panel discussion: Cybersecurity. *Standing Advisory Group Meeting* (PCAOB, Washington, DC).

PwC (2021) Stronger enforcement puts teeth in cyber and privacy rules. Accessed August 21, 2021, https://www.pwc.com/us/en/services/consulting/cybersecurity-privacy-forensics/library/cybersecurity-enforcement-financial-sector.html.

PwC (2022) Overseeing cyber risk: The board's role. Report, PwC Governance Insights Center, New York.

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* (September 25), https://www.wsj.com/articles/boards-still-lack-cybersecurity-expertise-70094266.

Sahin Z, Vance A (2025) What do we need to know about the chief information security officer? A literature review and research agenda. *Computers Security* 148:104063.

Saldaña J (2013) *The Coding Manual for Qualitative Researchers*, 2nd ed. (Sage Publications, Thousand Oaks, CA).

Schwartz-Ziv M, Weisbach MS (2013) What do boards really do? Evidence from minutes of board meetings. *J. Financial Econom.* 108(2):349–366.

SEC (2011) Cybersecurity. *SEC Division of Corporation Finance* (SEC, Washington, DC).

SEC (2018) *Commission Statement and Guidance on Public Company Cybersecurity Disclosures* (SEC, Washington, DC).

SEC (2021a) *Cybersecurity Risk Governance* (SEC, Washington, DC).

SEC (2021b) *SEC Announces Three Actions Charging Deficient Cybersecurity Procedures* (SEC, Washington, DC).

SEC (2021c) *SEC Charges Issuer with Cybersecurity Disclosure Controls Failures* (SEC, Washington, DC).

SEC (2021d) *SEC Charges Pearson Plc for Misleading Investors About Cyber Breach* (SEC, Washington, DC).

SEC (2022) *Proposed Rule: Cybersecurity Risk Management, Strategy, Governance and Incident Disclosure* (SEC, Washington, DC).

SEC (2023) *Final Rule: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure* (SEC, Washington, DC).

Sila V, Gonzalez A, Hagendorff J (2017) Independent director reputation incentives and stock price informativeness. *J. Corporate Finance* 47:219–235.

Suchman MC (1995) Managing legitimacy: Strategic and institutional approaches. *Acad. Management Rev.* 20(3):571–610.

Tidy J (2021) U.S. companies hit by 'colossal' cyberattack. Accessed July 19, 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* 34(1):199–230.

Tunggal AT (2021) Why is cybersecurity important. Accessed July 19, 2021, https://www.upguard.com/blog/cybersecurity-important.

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* (U.S. Department of the Treasury, Washington, DC).

U.S. Department of the Treasury (2020) *Consent Order* (U.S. Department of the Treasury, Office of the Comptroller of the Currency, Washington, DC).

Weisbach MS (1988) Outside directors and CEO turnover. *J. Financial Econom.* 20:431–460.

Wijen F (2014) Means versus ends in opaque institutional fields: Trading off compliance and achievement in sustainability standard adoption. *Acad. Management Rev.* 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. *J. Corporate Finance* 9(3):295–316.

Yin RK (2018) *Case Study Research and Applications: Design and Methods*, 6th ed. (Sage Publications, Los Angeles, CA).