PAMPLIN COLLEGE OF BUSINESS
VIRGINIA TECH

880 West Campus Drive
Pamplin Hall, Suite 1030
Blacksburg, Virginia 24061

September 8, 2022

Ms. Vanessa Countryman
Secretary
Securities and Exchange Commission
100 F Street NE
Washington, DC 20549-1090

Re: S7-09-22 Cybersecurity Risk Management, Strategy, Governance (RSG), and Incident Disclosure

Dear Ms. Countryman:

We are business professors with expertise in cybersecurity and corporate governance at the Pamplin School of Business at Virginia Tech. We write to comment on the proposed rule of "Cybersecurity Risk Management, Strategy, Governance (RSG), and Incident Disclosure" (hereafter "the proposal"), specifically Items D and E related to disclosures of cybersecurity governance and directors' cybersecurity expertise. We have conducted a study directly related to this proposed rule.

Our study is summarized in an article titled, "Why Corporate Boards Need More Cybersecurity Expertise," published in *The Wall Street Journal* (WSJ) on September 7 (online) and 9 (print), 2022, from which we excerpt below. Our full paper, on which the WSJ article is based, is attached to this letter. It is titled "Inexpert Supervision: Field Evidence on Boards' Oversight of Cybersecurity," and is currently under peer review at a leading accounting journal.

Below we briefly highlight our study and findings. We conducted a qualitative, interview-based field study with directors, chief information security officers (CISOs, or other similar security executives), and consultants that work with boards on cybersecurity of mid- and large-cap firms. We investigated how directors provide cybersecurity oversight and the role of expertise in determining its effectiveness. Overall, we found that "most boards lack adequate understanding of cybersecurity, and this substantially affects the quality of their oversight" (WSJ).

Specific findings relevant to this proposal include (excerpts from our WSJ article in quotations):

- "[L]ack of expertise leads to superficial, check-the-box oversight. For example, board members may simply not give adequate attention to cybersecurity, since directors naturally focus on things they know best. They may ask the CISO naive or off-the-shelf questions that don't cut to the heart of the company's cybersecurity risks."
- "When answers are provided, directors may not understand them, or be able to detect rosy framing or ask follow-up questions to probe if the CISO or their program needs a shift in direction."
- "[B]oards with low expertise tend to overrely on CISOs. Many CISOs must regularly educate the board about cybersecurity issues before they can be meaningfully discussed. [… this] limits what the CISO can report in the brief time allotted in board meetings. Worse, it can make the board members dependent on the CISO for their understanding of the issues at hand."

- "[M]any CISOs actively coach the board about what information the board should receive, what questions the board should ask, and what the target metrics for cybersecurity should be. This circular oversight, where the subjects of oversight (the CISOs) determine how they are overseen, lacks independence and is clearly problematic."
- "[M]ost CISOs we interviewed readily conceded that, given boards' lack of cybersecurity expertise, filtering out thorny issues in reports to the board is a temptation for them or their peers. In comparison, directors we spoke with largely said that CISOs wouldn't filter their reports this way, or that if they did, directors could detect their coverup attempts."
- Benefits of directors with cybersecurity expertise include that they "can talk with the CISO to fully understand issues and challenge the CISO's cybersecurity programs when needed. They can also be a tremendous asset to the CISO by acting as a go-between with the board and by lending political capital to the CISO's requests to the C-suite for resources and needed organizational changes."
- "[T]rue expertise—such as that gained through direct, hands-on experience managing cybersecurity—provides the most benefits. However, even modest investments in a board's expertise, such as cybersecurity training, can pay substantial dividends."
- Not all of our participants believe that boards need cybersecurity expertise as a director skill. Concerns include that directors with cybersecurity expertise may have little other value to the board, that other directors may over rely on the director with expertise, or that an expert director is more likely to micromanage the CISO.
- Despite these concerns, "the overall consensus was that expertise enables directors to provide proactive, value-added oversight of cybersecurity risk that wouldn't be possible without it."

Our findings underscore the importance of understanding the role of boards in cybersecurity oversight, and we agree that rules like S7-09-22 that the SEC is proposing will improve transparency of cybersecurity governance. We refer you to both our WSJ and full academic articles. We hope that this timely study provides useful insights to the Commission as it weighs the need for further disclosures related to director cybersecurity expertise and the board's role in cybersecurity risk oversight.

Sincerely,

Michelle Lowry
Assistant Professor | Virginia Tech | Accounting and Information Systems
https://acis.pamplin.vt.edu/directory/michelle-lowry.html

Marshall Vance
Assistant Professor | Virginia Tech |Accounting and Information Systems
https://acis.pamplin.vt.edu/directory/vance.html

Anthony Vance
Professor | Virginia Tech |Business Information Technology
https://anthonyvance.com

Inexpert Supervision:

Field Evidence on Boards' Oversight of Cybersecurity

Michelle R. Lowry
Virginia Tech
[redacted]

Anthony Vance
Virginia Tech
[redacted]

Marshall D. Vance
Virginia Tech
[redacted]

December 22, 2021

Acknowledgements: We are grateful to the board directors, cybersecurity executives, and consultants who agreed to participate in this research. We appreciate comments from Chris Barhorst, France Bélanger, 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 2021 BYU Accounting Research Symposium, Miami University, the University of Jyväskylä, the University of South Florida, and Virginia Tech.

Inexpert Supervision:

Field Evidence on Boards' Oversight of Cybersecurity

Abstract

We conduct an interview-based field study to investigate how directors provide cybersecurity oversight and the role of expertise in determining its effectiveness. Our interviews suggest that directors' cybersecurity expertise is an important determinant of oversight effectiveness, primarily through increasing directors' attention to cybersecurity issues and enabling them to ask incisive questions of management. Moreover, in the absence of board expertise, directors rely heavily on chief information security officers (CISOs) to "coach" them on cybersecurity concepts, third-party validation, and even the process of cybersecurity oversight itself. Thus, a lack of board expertise can result in circular governance between the board and management, whereby the terms of oversight are largely dictated by the supposed subjects of that oversight. Further, our CISO participants believe their peers filter reports to the board to obfuscate potentially damaging information, and that boards lacking cybersecurity expertise are not able to detect such filtering.

Keywords: Corporate governance, boards of directors, board oversight, risk oversight, cybersecurity risk, agency theory, self-efficacy theory, qualitative field study

Inexpert Supervision: Field Evidence on Boards' Oversight of Cybersecurity

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

SEC Commissioner Robert Jackson, 2018

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

Former NASDAQ Board Director

I. INTRODUCTION

Boards of directors have a fiduciary duty to oversee firms' management of material risks, which increasingly include risks related to cybersecurity.[1] Reflecting an expectation for boards' oversight, the SEC states that firms should disclose details about the board's role in overseeing cybersecurity to enable "investors to assess how a board of directors is discharging its risk oversight responsibility in this increasingly important area" (SEC 2018, 18). While regulators and investors emphasize that boards should provide substantive cybersecurity oversight (e.g., Aguilar 2014; CII 2016), cybersecurity may pose unique oversight challenges to boards due to their relative unfamiliarity with the subject matter, its technical nature, and its recent emergence as a key board responsibility.

Proficiency in cybersecurity is not a central qualification for most board members (Larcker, Reiss, and Tayan 2017). Moreover, specific responsibility for cybersecurity oversight is typically delegated to the audit committee (EY 2020), which is primarily focused on financial reporting. Board directors themselves have expressed reservations about boards' ability to adequately oversee cybersecurity (PwC 2019; Cheng, Groysberg, Healy, and Vijayaraghavan 2021). For example, a survey of corporate directors suggests that 52 percent of public company directors are

[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).

not "confident that they sufficiently understand cyber risks to provide effective cyber-risk oversight" and 42 percent do not believe "their boards collectively know enough about cyber risk to provide effective oversight" (National Association of Corporate Directors (NACD) 2018).

To provide large-sample evidence of the cybersecurity gap among public company boards, we investigate the prevalence of cybersecurity among director skill sets disclosed in proxy statements. Regulation S-K requires that firms disclose information about directors' "particular areas of expertise or other relevant qualifications" (Item 401(e) of Regulation S-K). We examine 1,000 proxy statements from a random sample of the Russell 3,000 and find that just under 15 percent of firms disclose that any of their directors had cybersecurity expertise. The general scarcity of cybersecurity expertise[2] at the board level raises the following important research questions: (1) How do directors provide cybersecurity oversight? and (2) How does director expertise influence the effectiveness of cybersecurity oversight?

To investigate these questions, we perform a qualitative field study using methods well suited to gaining in-depth insight into boards' monitoring activities and decision making (Yin 2018) and that have been used in recent accounting research (e.g., Bills, Hayne and Stein. 2018; Hayne and Vance 2019; Dodgson, Agoglia, Bennet and Cohen 2020).[3] We conduct 30 interviews with board directors and cybersecurity executives who interface with boards, incorporating the perspectives of those who conduct oversight and those who are overseen. We also interview consultants who support boards' governance of cybersecurity to provide an outside view of the board–management relationship in cybersecurity oversight. We follow guidance on positivist field

[2] Expertise and experience are closely related, although expertise implies domain-specific knowledge from both experience and ability (Bonner and Lewis 1990). Therefore, we generally use the term "expertise" because it more precisely refers to an individual's capability. We recognize that director cybersecurity expertise is relative and falls on a continuum. For ease of exposition, in this paper we refer to cybersecurity expertise simply as "expertise."
[3] Approval for this research using human subjects was granted by the institution at which the research took place.

research (Malsch and Salterio 2016), and draw on theory to help explain our field observations. While agency theory predicts that boards provide substantive and independent oversight of management (Fama 1980), self-efficacy theory (Bandura 1982, 2001), which addresses the socio-behavioral effects of expertise, suggests that a lack of expertise may lead to insufficient attention to cybersecurity issues, as well as to excessive reliance on management.

Our interviews suggest that the level of individual directors' cybersecurity expertise is an important determinant of the effectiveness of board oversight. Consistent with self-efficacy theory, cybersecurity expertise influences the attention given by boards to cybersecurity issues; when boards lack directors with cybersecurity expertise, they are less likely to substantively address cybersecurity during board meetings. Participants described that, in the absence of expert directors, boards may adopt a compliance attitude to "check a box" by receiving cybersecurity reports without significantly engaging with cybersecurity executives. In addition, our interviewees shared that cybersecurity expertise affects the quantity, quality, and depth of the questions that directors ask cybersecurity executives as well as their ability to meaningfully respond to answers received. We find that when inexpert boards do engage with cybersecurity executives, they often ask superficial questions (such as "How are we doing?") or reactive questions (such as "Could that happen to us?" in response to a cyber incident in the media).

Further, consistent with self-efficacy theory, we find a lack of cybersecurity expertise leads boards to rely heavily on the chief information security officer (CISO) to coach them on cybersecurity concepts, risks, program objectives, and even the process of cybersecurity oversight itself.[4] This reliance on management inhibits the board's ability to provide an independent assessment of cybersecurity risk or to provide incremental value in their oversight. In contrast to

[4] For ease of exposition, we refer to senior executives with direct responsibility over cybersecurity collectively as "CISOs".

perspectives from agency theory, which emphasizes conflicts between boards and managers and the need for the former to independently verify the latter's efforts (Fama 1980), we find that many directors downplay the potential for conflict but rather emphasize that the board and managers are part of the same team. However, our CISO-participants were more forthcoming about potential conflicts, such as a CISO reporting a more favorable view of their performance and the firm's overall cybersecurity position to the detriment of the firm. In particular, many CISOs believe that filtering negative aspects from reports is a common practice. Moreover, CISOs believe that boards lacking cybersecurity expertise are not able to detect such filtering.

While specific responsibility for cybersecurity is typically delegated to the audit committee, interviewees indicate that one or two directors (not necessarily a member of the delegated committee) may organically volunteer to take on added oversight responsibilities beyond their formal role. Such initiative is based on a director's personal interest or their having more expertise in cybersecurity relative to peers on the board. These voluntary activities include engaging with the CISO outside of regular board meetings, acting as an intermediary between the CEO and the CISO, advocating for increased budgetary spending on cybersecurity, and previewing the CISO's report before it is presented to the full board. Thus, our findings indicate that substantive oversight can be organic and ad hoc rather than planned and assured through formal processes.

Although interviewees were unanimous in recognizing benefits of expertise in improving oversight, they did not uniformly perceive a need to appoint a bona fide cybersecurity expert to the board. Some participants expressed the view that general business and risk management experience were sufficient. In contrast, others strongly called for directors with genuine cybersecurity expertise and argued that a lack of expertise potentially exposes firms to significant risk. In terms of what qualifies a director as having relevant "expertise," our interviewees shared

that direct experience working in or overseeing a cybersecurity function is necessary, whereas serving on a cybersecurity-focused committee or receiving short training or director-focused cyber certification (although beneficial) is insufficient.

This paper makes several contributions. We provide field evidence for the influence of director expertise on boards' attention and ability to perform their monitoring function. In doing so, we answer the call for research on the challenges that boards face in conducting oversight and the board characteristics and activities that lead to differential oversight effectiveness (Cheng et al. 2021). Although our focus is on boards' oversight of cybersecurity, we contribute to the broader corporate governance literature examining the influence of directors' subject-matter expertise on related outcomes (e.g., McDaniel, Martin, and Maines 2002; Cohen, Hoitash, Krishnamoorthy, and Wright 2014; Agrawal and Chadha 2005; Fich and Shivdasani 2007; Xie, Davidson, and DaDalt 2003; Abbott, Parker, and Peters 2004; Baugh, Hallman, and Kachelmeier 2021). We complement these archival studies by opening the "black box" of board oversight and providing rich narrative examples of how directors' priorities and monitoring activities differ based on expertise.

Our study has implications for the growing body of research in accounting and related fields on the antecedents and effects of cybersecurity incidents (Banker and Feng 2019; Huang and Wang 2021). We provide field evidence that, in the absence of expertise, boards may rely excessively on management such that the terms of oversight (e.g., reporting content, objectives, and performance metrics) are largely dictated by the executives who are supposed to be the subjects of that oversight. Such circular governance appears unlikely to effectively mitigate agency conflicts and potentially exposes firms to an increased risk of cybersecurity failures. Accordingly, we contribute to the debate on whether cybersecurity expertise is needed at the board level (Larcker et al. 2017;

Ferracone 2019), and we expect that our findings will provide useful inputs into regulator and market participants' board composition decisions relative to cybersecurity expertise. More broadly, an implication of our findings is that boards without sufficient domain-specific expertise are unlikely to fulfill the monitoring role emphasized in the agency-based perspective of corporate governance.

We also contribute to the literature on the disclosure of cybersecurity issues (Amir, Levi, and Livne 2018; Ashraf 2021). In its recent guidance, the SEC specifically stated that "the development of effective disclosure controls and procedures is best achieved when a *company's directors* … are informed about the cybersecurity risks and incidents that the company has faced or is likely to face (SEC 2018 p. 4, emphasis added). Further, cybersecurity risk governance and disclosure continue to be a high priority for SEC rulemaking (SEC 2021a, 2021b, 2021c, 2021d). Our evidence suggests that, without expertise, the board is less likely to be meaningfully informed about cybersecurity risks; hence, related disclosures may be less informative to market participants.

Finally, we shed light on what constitutes "expertise" in the context of boards' responsibility in overseeing cyber risk. In the U.S., Congress is currently considering legislation requiring firms to disclose whether they have a board member with cybersecurity expertise (S.808 2021). The language of this bill mirrors that of the Sarbanes-Oxley Act (SOX), which requires firms to disclose the presence or absence of a financial expert on the board (U.S. Congress 2002). As was the case with defining financial expertise for SOX purposes (SEC 2003), what it means for a board member to be an "expert" in the cybersecurity domain is likely to be a controversial issue. We contribute by providing field evidence for what directors, executives, and consultants believe is needed in terms of cybersecurity expertise on the board.

II. BACKGROUND AND RELATED THEORY

Background

Cybersecurity incidents are increasingly prevalent and cause trillions of dollars in estimated losses annually (Fox 2021). Negative consequences of cybersecurity incidents include interruptions to operations, reputational costs, worse loan terms, and loss of firm market value (Huang and Wang 2021; Kamiya, Kang, Kim, Milidonis, and Stulz 2021; Tidy 2021; Tunggal 2021). Consequently, cybersecurity risk management is increasingly viewed as critical to firms' success (Doan 2019; KPMG 2021), with firms spending in excess of $150 billion annually on cybersecurity, a figure projected to increase to well over $200 billion by 2025 (Gartner 2021).[5] However, experts believe these financial investments are often in the wrong security initiatives, underscoring the need for boards to oversee cybersecurity investments to ensure that they provide value to shareholders (Morgan 2019; ISA and NACD 2020) .

Reflecting these trends and concerns, there have been numerous calls for board-level oversight of cybersecurity risk. For example, the Council of Institutional Investors (CII) states that "[e]ffective cybersecurity risk management starts with the board" (CII 2016, 2), and the Federal Trade Commission (FTC) asserts that "data security begins with the Board of Directors, not the IT Department" (FTC 2021). Moreover, oversight of cybersecurity has been a point of emphasis for the SEC, with Chairman Robert Jackson calling the rising cyber threat "the most pressing issue in corporate governance today" (Jackson 2018) and Chairman 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 has issued guidance that boards should explain in the proxy statement (DEF 14A) their "role in overseeing the management" of

[5] A recent survey by RBC Global Asset Management found cybersecurity to be institutional investors' top concern among environmental, social, and governance (ESG) issues (RBC 2019).

cybersecurity risk and how they "engag[e] with management on cybersecurity issues" (SEC 2018, p. 18), and cybersecurity risk governance continues to be a high priority for SEC rulemaking (SEC 2021a).

Regulators and legislators increasingly require boards to oversee cybersecurity. In 2001, in accordance with the Gramm-Leach-Bliley Act (GLBA), the U.S. Treasury's Office of the Comptroller of the Currency (OCC) issued cybersecurity standards for banks, requiring 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). Notably, the OCC specifically cited the failure of Capital One's board to provide effective cybersecurity oversight as a key reason for levying an $80 million fine in connection with Capital One's 2019 data breach (U.S. Department of the Treasury 2020). The New York Department of Financial Services (NYDFS) has issued rules for financial services firms operating in New York to require boards to receive reports from cybersecurity management at least annually (s 500.4(b) 2017) . This same regulation has since become law in 13 states for licensed insurance companies (Blosfield 2021) and has been proposed by the FTC in its amendments to the Safeguards Rule governing financial institutions under the GLBA (FTC 2019). Further, it is likely that regulators of other industries will adopt rules such as those of the OCC and NYDFS in the future (PwC 2021).

Despite the urgency of effective cybersecurity programs and the expectations for directors to oversee them (SEC 2018), survey evidence suggests that directors do not have sufficient expertise with which to provide adequate oversight of cybersecurity risk (NACD 2018; PwC 2019). For example, in their survey of 577 U.S. public company directors, Cheng et al. (2021) find that directors perceive cybersecurity to have the *lowest* level of board effectiveness among the 19

responsibility areas considered, and the authors suggest that the low effectiveness in this area is due to limited board-level experience or expertise.

Theoretical lenses

We follow Malsch and Salterio's (2016) suggestions for the use of theory in positivist field research. First, we use investors' and regulators' expectations and standards discussed above as "normative theory" (Malsch and Salterio, 2016, 5), which serves as a baseline against which practices observed in the field can be evaluated. Second, we use theories from related disciplines to form expectations against which to compare our findings. Agency theory (e.g., Jensen and Meckling 1976; Fama and Jensen 1983; Eisenhardt 1989) is the dominant lens through which corporate governance is viewed in the accounting and finance literatures (Beasley, Carcello, Hermanson, and Neal 2009), particularly as it relates to boards' monitoring (as opposed to advising) role.[6] We therefore use an agency perspective as a starting point from which to develop expectations for how boards conduct cybersecurity oversight. We also incorporate perspectives from self-efficacy theory to generate expectations for how cybersecurity expertise influences oversight.

Agency Theory Perspective

Under an agency perspective, top managers may not act in the best interests of shareholders due to insufficient ability or conflicting preferences (or both). For example, a CISO may prefer to shirk rather than incur personal cost from effort or may select inefficient cybersecurity investments representing pet projects. A fundamental tenet of agency theory is that firms seek to mitigate agency costs by separating decision management from decision control, and the board of directors

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

serves as the "apex" of the decision control systems (Fama and Jensen 1983, 323). Due to the potential for conflicts (and resulting costs) between shareholders and managers, agency theory suggests that the board's "most important role is to scrutinize the highest decision makers within the firm" (Fama 1980, 294). Hence, agency theory predicts that directors will be diligent monitors of material firm risks, including cybersecurity risks.

Domain-specific expertise is increasingly recognized as important for boards to fulfill their intended monitoring role (Hillman and Dalziel 2003; Hambrick, Misangyi, and Park 2015). The role of a board's financial expertise in particular has generated significant academic attention following the Sarbanes Oxley Act of 2002, which requires firms to disclose whether their audit committee has a financial expert. Studies show that financial expertise is positively associated with financial reporting quality and related outcomes (McDaniel et al. 2002; Xie et al. 2003; Bédard, Chtourou, and Courteau 2004; Abbott et al. 2004; Agrawal and Chadha 2005; Krishnan 2005; Goh 2009; Hoitash, Hoitash, and Bedard 2009; Lisic, Myers, Seidel, and Zhou 2019), and that market participants react favorably when a financial expert is appointed to the audit committee (DeFond, Hann, and Xuesong 2005). Collectively, these studies suggest that financial expertise enhances the extent to which boards fulfill their oversight responsibilities. As with financial reporting, cybersecurity is a technical domain, and thus, boards' oversight of a firm's cybersecurity program may similarly benefit from (or even necessitate) domain-specific expertise.

The agency perspective of corporate governance generally assumes the board possesses sufficient expertise to provide an independent[7] check on management (e.g., Fama and Jensen

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

1983). In contrast, drawing on resource dependence theory, Hillman and Dalziel (2003) argue that boards vary in their expertise (and human capital more generally), which in turn explains variations in boards' monitoring effectiveness. From a resource dependence perspective, when the board possesses sufficient domain expertise, we might expect vigilant, independent monitoring, as predicted by agency theory. However, when the board lacks such expertise, boards may not provide substantive oversight (Hambrick et al. 2015). While resource dependence theory highlights the importance of boards' human capital, it does not provide specific insight into how oversight may be affected by low capital. Thus, below we draw on self-efficacy theory to develop richer expectations for the effect of low cybersecurity expertise on boards' oversight activities.

Self-Efficacy Theory Perspective

Self-efficacy refers to "a set of beliefs about the ability to coordinate skills and abilities to attain desired goals in particular domains and circumstances" (Maddux and Kleiman 2020, 3). While individuals may possess generalized self-efficacy, domain-specific efficacy is more predictive of behavior in specific circumstances (Bandura 1997; Maddux and Kleiman 2020). Further, the "most potent and salient" source of self-efficacy beliefs is prior experience and performance in a task domain (Agarwal, Sambamurthy, and Stair, 2000, 419). Thus, we expect that directors with more cybersecurity expertise tend to have greater self-efficacy in the cybersecurity domain. A central idea from self-efficacy theory is that beliefs about capabilities are a primary basis of action (e.g., Bandura 1977; Bandura 1997; Maddux and Kleiman 2020), and prior research finds that self-efficacy is associated with intrinsic interest, activity, effort, and task persistence (Gist 1987; Cervone and Peake 1986; Bouffard-Bouchard 1990; Compeau and Higgins

1995).[8] The effects of self-efficacy may be particularly strong in a governance setting, because directors face time constraints and must choose the corporate issues on which to focus (Field, Lowry, and Mkrtchyan 2013). Consistent with this, Gendron and Bédard (2006), in the context of financial expertise, suggest that formal competencies may produce self-confidence, which leads directors with expertise to engage more on issues related to their background. Based on the foregoing, in the absence of expertise we expect boards to devote insufficient time and attention to cybersecurity oversight activities.

Self-efficacy theory also suggests that low expertise can inhibit effective cybersecurity oversight due to an increased reliance on cybersecurity executives. As noted above, agency perspectives of governance emphasize conflicts with management and hence the need for independent scrutiny by the board. However, self-efficacy theory predicts that individuals with low perceived efficacy (i.e., low domain expertise) are more likely to cede control to others who they perceive as having more efficacy, resulting in "a vulnerable security that rests on the competencies and favors of others" (Bandura, 1982, 142). This may result in low-expertise directors excessively deferring to their board colleagues who they perceive as having more cybersecurity expertise. Another possibility is that the board (individually or collectively) will resort to "proxy control" (Bandura 1982, 1997, 2001; Xu, Teo, Tan, and Agarwal 2012), ceding their duty to establish an independent assessment of the firm's cybersecurity program to management or cybersecurity consultants.

In summary, investors and regulators have repeatedly emphasized their expectations that boards oversee cybersecurity risk. Agency theory suggests that boards will recognize the potential

[8] In the accounting literature, self-efficacy has been shown to be a determinant of appropriate audit system use (Dowling 2009) and auditor judgements (Iskandar, Sari, Mohd-Sanusi, and Anugerah 2012). Self-efficacy theory is widely used in information systems research (e.g., Yoo, Goo and Rao 2020).

for agency conflicts and endeavor to provide independent, substantive oversight to ensure that the firm's cybersecurity program reflects shareholders' interests. However, many boards lack cybersecurity expertise, which may reduce a board's ability to provide such oversight and may result in low attention to cybersecurity issues, or excessive reliance (in place of scrutiny) on management as predicted by self-efficacy theory. Table 1 summarizes the theoretical perspectives we consider in this study. Given the current expertise gap in most firms, our primary aim is to understand how boards conduct cybersecurity oversight and how cybersecurity expertise influences the nature of their oversight.

III. METHOD

We follow best practices for positivist, qualitative field study methods from recent accounting research to investigate our research questions (e.g., Malsch and Salterio 2016; Bills et al. 2018; Hayne and Vance 2019; Dodgson et al. 2020; Free, Trotman and Trotman 2021). We use 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). Thus, qualitative methods were required to open the "black box" of boards' governance of cybersecurity, to understand how directors perform this fiduciary responsibility.

To explore possible themes, theories, and issues relevant to cybersecurity oversight, we reviewed SEC and PCAOB reports and guidance on cybersecurity oversight, regulatory cybersecurity roundtables, and practitioner and academic guidance (e.g., IIA 2010; SEC 2011; SEC 2018; PCAOB 2018; and NACD 2020). We also conducted preliminary interviews with professionals about the challenges boards face in their cybersecurity oversight. This initial field

work helped us to establish our theoretical lens for our study and to prepare an initial interview script (Yin 2018).[9]

Sampling Strategy

We conducted 30 interviews with 27 individuals belonging to three groups of professionals: board directors (11 participants), cybersecurity executives (9 participants), and senior-level consultants who advise boards on cybersecurity issues (7 participants).[10] The three participant types allowed us to triangulate our findings by obtaining varied perspectives of the parties involved in boards' oversight of cybersecurity (Miles, Huberman, and Saldaña 2020). Further, this sampling approach allowed us to compare and contrast responses across each group. In contrast to experimental and archival methods that make statistical inferences, our sample size was not determined by achieving a level of statistical power. Instead, we continued our snowball sampling process until the point at which novel insights were no longer obtained (i.e., we reached theoretical saturation; see, e.g., Morse 1995; Malsch and Salterio 2016).[11]

Our sampling approach yielded a participant group with diversity across a number of dimensions, as summarized in Table 2.[12, 13] Panel A shows that, among the 11 directors, five had "low," three had "medium," and three had "high" cybersecurity expertise. For the board members

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

[10] Note that three participants belonged to more than one group. Also, three other participants were interviewed twice to further explore themes raised in the initial interview.

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

[12] We restricted our interviews to those affiliated with mid- to large-cap companies because we expect these organizations are more likely to have a developed cybersecurity function.

[13] Two directors and three executive participants represent large private firms. Surprisingly, we did not find significant variation in the cybersecurity governance process between publicly- and privately-held firms. Specifically, for the participants who have experience with both public and private boards (Director-4, Director-5, Executive-5), we directly asked about the differences. We were told the differences, if any, were minimal, and interviewees indicated cybersecurity oversight in particular is similar.

we interviewed, all but two had delegated responsibility for cybersecurity as part of their membership of the audit committee or another committee tasked with overseeing cybersecurity in at least one of their companies.[14] The mean (median) number of director positions held by our director-participants was 3.1 (3). Panel B presents information regarding executive participants. While the executive titles varied, all participants were directly responsible for cybersecurity and reported to the board. The directors and executives represent both high- and low-technology industries. Panel C provides information on our consultant interviews. We interviewed senior-level consultants across a range of firms that provide cybersecurity consulting services to boards, including large technology solutions firms, the Big-4, and specialized consulting firms.

Interviews

At least two researchers participated in each of the 30 interviews, which were conducted by phone or video calls and lasted an average of 52 minutes. We audio-recorded and professionally transcribed all but four of these interviews. A graduate research assistant then reviewed each transcript against the corresponding audio recording to ensure accuracy. For the four interviews in which participants preferred not to be recorded, one researcher or a graduate research assistant took careful notes while two researchers conducted the interviews. Prior to each interview, we reviewed the participant's biographical information available from LinkedIn and any online biographies. For interviews with directors and cybersecurity executives, we also reviewed news articles, proxy statements, and annual reports relating to firms associated with the interviewees.

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

[14] 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).

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

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 we then narrowed down based on thematic overlap to form our initial codebook with definitions. These codes broadly included dimensions such as 1) the cybersecurity governance process, 2) directors' attitudes toward cybersecurity, 3) directors' cybersecurity expertise, and 4) interactions between directors and cybersecurity executives.

Next, all three researchers independently coded each of the interviews. In this phase of the analysis, we continued to generate and discuss potential new codes (initial coding), and 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 and especially relationships between codes (Saldaña 2013). After each interview was coded, each researcher independently wrote a memo of the main theoretical takeaways from the interview and of the new codes proposed. We then discussed major themes and codes of that interview.

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). With a finalized codebook, two researchers independently coded each interview once again to obtain a Cohen's kappa (κ) score as a measure of agreement among the researchers. Overall, we obtained a κ score of 0.63, indicating good agreement among the research team (Cohen 1960).

We also 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).

IV. FINDINGS

Before proceeding with our qualitative findings, we first report results from an analysis of proxy statements for a random sample of 1,000 firms from the Russell 3000 Index to assess the scale of the cybersecurity expertise gap at the board level for U.S.-listed firms. Specifically, we examine the prevalence of cybersecurity among directors' disclosed skills and qualifications,

which firms are required to describe under Regulation S-K.[15] We find that only 14.7 percent of firms disclosed at least one director with cybersecurity or related skills and experience. In contrast, every firm disclosed at least one board member with financial or accounting skills. Additionally, only 13.2 percent of the firms referenced experience related to cybersecurity or privacy in the biographies of board members. This analysis reinforces the surveys cited above (e.g., NACD 2018; PwC 2019; Cheng et al. 2021) and provides large-sample evidence of the cybersecurity expertise gap at the board level. Given the expectations of regulators and investors that boards oversee cybersecurity risk, this apparent expertise gap motivates our qualitative analysis of the role of expertise in cybersecurity oversight.

How Does Expertise Affect Boards' Cybersecurity Oversight?

In the following section, we describe our field study findings on how director expertise influences oversight activities and the resulting oversight effectiveness, with additional selections of supporting interview evidence presented in Table 3.

The Influence of Expertise on Attention

Throughout our interviews, directors acknowledged the board's oversight responsibility for cybersecurity risk and emphasized the importance of effective cybersecurity. At the same time, participants shared that the focus on cybersecurity varies across and within boards. At the low end of engagement, the board may passively receive reports from cybersecurity management. For example, a CISO described his/her limited role in board meetings as follows:

> *Every year so far, I have been asked to come on site for the board meeting. Then, they decided that there were other more important things to discuss, and so I was thanked for my time but taken off the agenda. . . .I never presented, I was always sent away. I don't even know how they understood [the report]. I just heard "thank you" second hand.* (Executive-5)

[15] We searched proxy statements from the 2020 proxy season for keywords "security," "privacy," "cyber," "CISO," and "CSO" in board skill matrices and director biographies.

Similarly, a consultant shared the limited focus on cybersecurity he/she had observed on some boards: "[Some boards] aren't very inquisitive. They don't really care. They'd like to see some metrics, but the attention in the meeting is elsewhere" (Consultant-3).

Several participants shared that board attention to cybersecurity is motivated by and limited to compliance concerns (Consultant-1, Director-9, Consultant-3, Consultant-4). A director, commenting on the compliance-driven approach he/she perceives from other boards, described it as, "They had to get a presentation about it. Let's check that box" (Director-9). A consultant explained, "Their 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" (Consultant-4). This tendency toward a compliance orientation appears inconsistent with regulators' expectations and agency theory that boards will provide substantive oversight.

With less engaged boards, attention is often reactive, piqued by cybersecurity incidents. CISOs described receiving many more questions about cybersecurity after prominent reports of breaches in the business press. Such external cyber incidents serve as a "wake-up call" (Director-5), wherein board members are then prompted to ask, "Could that happen to us?" (Director-3, Director-5). A consultant described how interest in cybersecurity can quickly change 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" (Consultant-3).

In contrast, many interviewees indicated that cybersecurity expertise is an important determinant of increased attention to cybersecurity risk. For example, directors with more cybersecurity expertise feel more comfortable engaging with management on cybersecurity issues. A director suggested that board members will naturally give more focus to the areas related to their

backgrounds, explaining, “I will always lean into the things that I know. As a director… I’m drilling into things that I know a lot about” (Director-7). Another director, noting that board meetings cover many topics for oversight, said, “People who are comfortable with certain subjects kind of jump in at that time” (Director-8). Similarly, after pointing out that cybersecurity is outside of the expertise of a typical director, another director told us, “It’s definitely human nature to spend a lot more time on things that you’re more comfortable in. I think if you were to simply measure the amount of time boards spend talking about cyber risk compared to financial risk, you’d find it’s a tiny fraction” (Director-9). Thus, consistent with predictions from self-efficacy theory, our findings suggest that expertise is an important determinant of cybersecurity oversight effectiveness because it determines how much attention is given to cybersecurity during board meetings.

How Expertise Influences the Quality of the Questions Asked

Even for boards that take time during board meetings to engage with the CISO, the effectiveness of the questions varies with expertise. Table 4 presents interviewee-provided examples of questions that directors pose, categorized as superficial or substantive. Questions are more likely to be “basic” (Executive-4) when directors have little expertise with cybersecurity. In contrast to the superficial questions posed by inexpert directors, respondents frequently shared that directors with more expertise are able to ask higher-quality questions during board meetings. Many respondents stated that cybersecurity knowledge or domain expertise allows directors to ask “better” (Executive-4), “good” (Director-2, Executive-2, Director-5), “intelligent” (Executive-2, Consultant-3), “tough” (Executive-8), or “the right” (Consultant-1, Director-7, Executive-3, Director-8, Director-11, Consultant-7, Executive-8) questions. Several interviewees offered analogies to financial expertise. For example, “It’s no different from having a financial expert on

the board. If you have a financial expert on the board, they at least know what questions to ask the CFO to give themselves comfort that the books aren't being cooked" (Director-11).

A director with high cybersecurity expertise offered examples of probing, more sophisticated questions, and then noted 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" (Director-11). The difference in question quality based on expertise levels was explained by a self-described "inexperienced" director who referred to a colleague with more expertise: "His questions just might be a little bit better because he knows where some of the stumps are underneath the water" (Director-8). A consultant elaborated on how expertise levels result in different questions, with a specific example:

> *[A board member with cybersecurity expertise] will ask technical questions. They'll be aware of things going on in the industry. And they'll say, what sort of CASB [Cloud Access Security Broker] do we have, and is it good enough? And the other members of the board are going to say, what the [expletive] is a CASB? So it's a big difference.* (Consultant-3)

A cybersecurity executive, noting the role of technical expertise in raising a director's ability to ask questions, suggested, "They're going to have a completely different level of expertise and knowledge and are going to be much more thorough in asking probing questions" (Consultant-5).

Relatedly, several respondents described a synergistic outcome from a board having a member with cybersecurity expertise, whereby the director with expertise is able to initiate a line of questioning that the inexpert directors would not have thought to ask, but once the conversation has been started, the other members can use their general business experience to weigh in on the topic and provide additional oversight. "I would not characterize it as leaning on [the board expert] as much as feeding off of him and benefiting from his experience and input" (Director-8). This director continued:

> *It actually prompts further discussion because if somebody asks a question that you hadn't thought of yet, that might lead you to think of a follow-up question, and I think that's when the board's working at its best, is when the conversation gets started because of somebody's experience, and then that triggers additional questions.* (Director-8)

The foregoing examples clearly highlight the implicit assumption of agency theory that directors have sufficient expertise to provide substantive, independent oversight (Fama and Jensen 1983; Jensen 1993). From the above examples, expertise leads to higher question quality and more meaningful oversight. In cases where expertise is lacking, oversight is shallow and perfunctory, contrary to the expectation of agency theory.

Expertise Influences How Answers Are Received

Just as expertise enables directors to ask better questions, expertise similarly allows directors to understand the answers they receive from technical managers. CISOs may respond to a question at a technical level that many inexpert directors would not be able to understand or interpret, and thus be incapable of assessing the adequacy or the implications of the CISO's response. Reflecting on this problem, a consultant observed that board members without expertise may get "lost" during management's cybersecurity briefings. He explained:

> *Frankly, CISOs and the typical person you find on those boards speak two different languages. The CISO speaks a systems engineering or computer science language that come out of a computer science or systems engineering degree. And the people typically on the boards are lawyers or MBAs. And they speak an entirely different language. So that frequently, 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. That's a real critical problem. So, it's important that you have someone on the board who actually speaks "geek," who actually knows what is being said and can have a dialogue, and can ask questions. Because otherwise, it's kind of a dialogue of the deaf.* (Consultant-3)

Further, respondents described that additional expertise is particularly important for enabling a director to ask valuable follow-up questions. Just as a person learning a foreign language

can ask a simple question and not understand the response, so too can low expertise prevent the board from having a meaningful dialogue with the CISO. A consultant explained:

> *It's not the first question that you ask, because you can download the dummy's guide to cybersecurity. It's the second, and third, and fourth, and fifth questions that go off of the branching logic, based on how the CISO is providing his or her updates.* (Consultant-7)

Our findings of the role of expertise in the quality and quantity of questions, and in attendant question-driven dialogue, is consistent with directors with high self-efficacy exhibiting stronger commitment and persistence in their cybersecurity oversight.

The Relationship Between the Board and the CISO

Lack of Expertise Requires Coaching by CISOs

The participants with whom we spoke described CISOs providing a category of support activities to the board that we label "coaching." These activities include educating the board about cybersecurity and conditioning them regarding the content of information they should receive in reports and what level of risk is acceptable.

Educating the board. Several of the CISOs we interviewed indicated that they view educating the board as an important part of their responsibilities to "level set," get "on the same page," and provide "a common language" relative to cybersecurity (Executive-3, Director-7, Executive-9). For example, one CISO observed:

> *When I first joined… in terms of grade level, there was an elementary level of understanding [of cybersecurity on the board]. I met with and talked with each [board member] independently to understand their level. I immediately gauged that some had some knowledge, while others had none. Through the years, part of my job is to educate them… I call this "raising their cyber IQ."* (Executive-4)

CISOs described personally conducting "Security 101" (Executive-6) training as part of their regular meetings with the board as well as meeting informally with board members to answer their questions about cybersecurity concepts and current events. Often, directors use the Q&A period

of the CISO's presentation to ask "'educating themselves' kind of questions" (Executive-3), rather than questions specific to the state of the company's security program. Further, turnover on the board and time elapsed since the previous board meeting necessitates regular review of concepts previously taught. Current events, such as data breaches in the business press, are also frequently discussed, with directors seeking to learn the concepts involved and the implications for their organization. Even budgetary requests to purchase cybersecurity software or services often requires the CISO to instruct the board:

> *It's not like in a lot of cases, if you're saying, look, "we need new fire extinguishers." 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 or … mobile device management," now you may need to explain what that means, and why do you care, and what are the consequences."* (Consultant-1)

Although presentations to the board by various corporate officers can often include educational elements, one CISO describe the difference with cybersecurity in this way:

> *[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. And that in comparison, [cybersecurity is] a topic that everybody's trying to really figure out, "What does it mean?"* (Executive-1)

Conditioning the board. After providing a definition of cybersecurity, one CISO was asked whether the board shared this understanding. The CISO replied, "Yes, because I have conditioned them to that definition" (Executive-4). Conditioning goes beyond definitions to setting expectations for how a security program should function and for appropriate levels of risk. For example, one CISO presented the NIST Cybersecurity Framework to the board and explained, "This is what a good program should look like" (Executive-3). Another CISO set expectations for appropriate scores for a cybersecurity maturity model:

> *[T]here were more questions around risk and, "Why should we only be a three and a half versus a five? Why don't you want to be a five…?" You know, doesn't*

> *everybody want to have A's? But that's not how the model works. You don't need to be a five in everything. So we had to kind of explain that to them…"* (Executive-2)

One consultant compared this process of setting expectations to a negotiation with the board: "'We do not want to be the next Anthem,' they said. 'No breaches.' The CISO very wisely said, 'That is impossible, but what I can promise to you…'" (Consultant-7).

In cases of low expertise on the board, CISOs not only set expectations but also determine what type of information is reported to the board, because directors do not know what type of information about the cybersecurity program they would like to receive from management. For example, one CISO explained:

> *[T]he boards really don't know what they want to know, in what format. There's nothing that's been established, like in accounting or finance, where things seem pretty straightforward. … And so, we're all going through this process of developing "what should the board see?" and "what should they care about?" … It's probably a journey of, "Okay, what resonates with the board and helps them provide the best oversight?"* (Executive-3)

Further, one CISO described steering the board to a particular form of cybersecurity audit because "they didn't know what they were asking for" (Executive-5). In addition, CISOs described instructing the board about what types of questions are useful for the board to ask the CISO.

The coaching activities described above demonstrate the dependence of low-expertise boards on the CISO to learn what cybersecurity oversight should entail and how oversight should be conducted, including how to determine acceptable risk levels, what metrics to look at, what questions to ask, and whether to engage third parties to verify the firm's cybersecurity position. Thus, our interviews suggest that the 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. Overall, this dynamic does not appear consistent with expectations from agency theory that boards will provide independent oversight. Rather, consistent with self-efficacy theory,

our findings suggest that low expertise leads to boards effectively ceding key aspects of their oversight role to the CISO.

Expertise Enables Board Members to Detect False or Withheld Information

A manifestation of the agency conflict between the board and a CISO is the tendency of the latter to filter cybersecurity reports to improve the board's assessment of the CISO's performance. Due to the sensitive nature of this issue, we asked participants about their perceptions of whether this dynamic is common in other companies. There was variation among interviewees regarding the prevalence of CISOs filtering reports, with some expressing the opinion that filtering is human nature and thus widespread. A CISO explained that it was in his/her nature to be honest and forthcoming but reflected on other CISOs' tendencies to filter out negative information from reports to make themselves look better: "I know that happens, just because I hear [other CISOs] say those words: 'You got to craft the message to the board'" (Executive-1). When asked whether filtering by the CISO happens, a consultant flatly stated, "Oh, of course. All the time" (Consultant-3). Among the executives and consultants we interviewed, only one stated the belief that CISO obfuscation is not a potential concern, sharing, "I can only speak to my small inner circle of CISOs I know—they want to be transparent. They are not hiding things, I have never heard of that being done" (Executive-4).

To corroborate our interviewees' views that opportunistically filtering reports is a common practice, we surveyed an additional 33 cybersecurity executives.[16] In response to the question, "From your impression of firms in general, what percentage of CISOs filter their reports to the

[16] We administered the survey to members of Gartner's CISO Coalition, a network for collaboration and information sharing among CISOs and other cybersecurity executives.

board to make themselves or their superiors look better?" the mean (median) is 42 (40) percent of CISOs, and all but one respondent reported a nonzero percentage.[17]

We find that, compared to CISOs and consultants, directors more often view CISOs as unlikely or unable to obfuscate. Among the eleven directors we interviewed, five shared that filtering was unlikely to occur or otherwise downplayed the existence of a conflict with management. For example, one director commented, "I think most of the CISOs I have seen are like internal auditors. They're not trying to hide things" (Director-10). Another director similarly shared, "I would say [at our company], everybody wants to do the same thing. Because they know if there is a gap that could be a problem tomorrow. It could bring the company down. So, there's very little inclination to do anything other than use the data for good" (Director-2). Related to the lack of a perceived agency conflict, a director explained why he/she would not advocate hiring a third-party to independently verify the CISO's work: "I think you've got to work with the owner. If I tell you, 'You own this risk,' then I can't then go and say, 'I'm going to hire somebody else to see if you're doing your job.' I don't think that works. It's got to be a team approach" (Director-1). All three director participants with cybersecurity executive experience strongly acknowledged the potential for CISO obfuscation. One said, "I think there's always that risk and I think that a board should have a high awareness and concern for that." (Director-5).

Respondents suggested that board members' sophistication with cybersecurity is an important factor in limiting this behavior. A CISO candidly shared his/her experience under a prior CIO (who was above the CISO in the organizational hierarchy):

> *[The former CIO] always used his presentation to sell.… That is my perception of how it was. Paint your performance in the best possible light—that was my*

[17] 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, Bouffard, Piquero, and Craig 2016). In addition, asking about behavior of respondents' peers is a common way of reducing social desirability bias (Fisher 1993).

> *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.* (Executive-5)

When asked whether the expertise gap exacerbates the tendency to present a rosy picture of cybersecurity, this CISO responded, "If (the board) can't ask questions, then absolutely" (Executive-5). Another CISO described director expertise curbing filtering:

> *If we didn't have a person with the domain knowledge, it would be very easy to hide things and obfuscate things. Or, you know, you're going to sing your praises, right? …. Transparency is really, really important to us. But I definitely think it would be possible to not be transparent and to hide or obfuscate things, or bury risks that are uncomfortable or that you don't want to talk about.* (Executive-2)

Another respondent emphasized the importance of directors knowing "the right questions to ask, such that they can decipher truth from fiction or snow from reality and what the CISO or the CISO's advisors are telling him or her" (Consultant-7). A CISO described it this way:

> *I think [cybersecurity expertise] enhances oversight … It gives the board the ability to smell out a situation where management may be whitewashing a particular subject, or they might be trying to speak at a level that … really doesn't get to the root of a certain situation.* (Executive-3)

In summary, we find that, as emphasized by agency theory, conflicts do exist in the board–manager relationship. However, inconsistent with agency theory, we find that directors may not recognize managers' incentives or ability to obfuscate information. Moreover, when boards lack cybersecurity expertise, the potential for agency costs is greater. A director summarized the vulnerable position of a board lacking cybersecurity expertise. In contrast to the typically deep financial expertise that most boards possess, the comparative dearth of cybersecurity knowledge leaves boards having to rely on CISOs' reports based on "trust and faith":

> *[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. [Board members] don't know the metrics, they don't know the reports, they don't know the*

> *content, and they really are just having to take it mostly on trust and faith.* (Director-9)

Expertise Enables Board Members to Challenge the CISO

Related to the above, respondents explained that cybersecurity expertise enables a director to "know what good looks like" (Director-5, Consultant-7), and thus be better able to evaluate management's cybersecurity efforts and to "challenge" (Consultant-3, Executive-8) management on issues that arise. A consultant described this as, "They are going to 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" (Consultant-3). Another observed:

> *[Having a cybersecurity expert on board] really calls and exacts more of the CSO or CISO who is going into the event, 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.* (Executive-7)

Similarly, an executive described how, after the board appointed a new director with a "strong cyber background" for the first time, this savvy director could "challenge our CISO on materials and information being presented" (Executive-8). More broadly, cybersecurity expertise enables board members to assess the quality and/or fit of the CISO for the organization (Director-11). Although agency theory assumes boards will be an independent check on management, our participants suggest that expertise provides directors with both the motivation and the ability to move beyond symbolic oversight and instead provide critical feedback to cybersecurity executives.

Expertise Influences Directors' Proactive Engagement

Although much of the board oversight described by participants occurs during regular board meetings through formal reporting and questioning processes, our interviews revealed that a major form of substantive oversight can occur when directors voluntarily engage beyond formal processes, which we term "stepping up." This type of oversight is unstructured and self-selected

and most often undertaken by directors who have more expertise in cybersecurity (Director-2, Executive-2, Consultant-7).

Stepping up often involves reoccurring ad hoc conversations and meetings and information sharing between the proactive director and the CISO (Executive-1, Director-2, Executive-6, Consultant-3); these informal interactions foster both information sharing and relationship building. Other forms of stepping up include attending meetings beyond a director's assignments (Executive-1, Consultant-7), providing critical feedback on the cybersecurity program both at the oversight and management level (Director-1, Director-10, Executive-7, Executive-8), initiating engagements with cybersecurity consultants (Director-1, Executive-2, Consultant-3), acting as an intermediary between the CISO and the CEO (Consultant-3, Executive-8), questioning the CEO and other non-CISO executives about cybersecurity (Executive-2), increasing budgetary spending (Consultant-3), requesting additional information (Consultant-7), requesting specific benchmarking (Consultant-7), and previewing the CISO's report before it is presented to the board (Director-5).

A specific form of stepping up is a director choosing to take a "deep dive" into the firm's cybersecurity program (Executive-2, Director-5, Consultant-7). A deep dive is a focused period of learning about the firm's cybersecurity systems and issues, which can help the director have a better institutional understanding of the firm's specific cybersecurity risks, the programs being instituted, the investments in the program, and the activities and capabilities of management. One director who also has cybersecurity executive experience initiated one such deep dive:

> *As a sitting CIO and someone who has grown up in the cyber space, I certainly wanted to see a little more focus on that 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"…. I said, "You hired me for a*

> *reason. Here's my experience, and here's where things can go wrong. I'm not saying they have, but wouldn't you like to make sure?"* (Director-5)

Such deep dives tend to cause additional work for management and spur them toward improving their systems (Executive-2).

> *[Without the director that stepped 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 and bring that in. Because … it's not cheap. It costs a lot of money to have these guys come do this work. So yeah, I think we would be at a very different [place]...*
>
> *….You're forcing me to face the reality that I don't want to face, which was [Director-X] 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. I don't think we would have, if [the director] hadn't pushed us on that…. [I]t was just a ton of work by me and my team to move that one forward. But had we not done that, we wouldn't be where we are today.* (Executive-2)

While we document various forms of "stepping up" as a common organic oversight phenomenon, because this form of oversight is not embedded in governance processes, the more usual course is for directors with low expertise to perform superficial oversight (Consultant-1, Director-9, Executive-5, Consultant-3, Consultant-6, Consultant-7, Executive-8).

Altogether, our field evidence indicates that the relationship dynamics between the board and the CISO varies based on board cybersecurity expertise. In the case of low expertise, the relationship is more likely to be characterized by low oversight independence, with the board being guided by and over-relying on the CISO. With high expertise, high oversight independence is more likely, as indicated by the board proactively monitoring, advising, and providing substantive feedback to the CISO. Table 5 provides additional examples of interview evidence showing these relationship dynamics.

Is Cybersecurity Expertise Needed?

As described in the previous two sections, the benefits of board cybersecurity expertise for monitoring effectiveness were widely acknowledged by our interviewees. However, our respondents frequently pointed out that such expertise is lacking for most boards. For example, a CISO said that most boards' cybersecurity expertise is "woefully" inadequate (Executive-9). One consultant pointed to the "real naivety" of boards in terms of cybersecurity (Consultant-6), and another said that the average board rates a "3" on a cybersecurity expertise scale of 1–10 (Consultant-5). A board member with cybersecurity expertise observed:

> *[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… Let's make clear, most people on a board today…, if they have a technical background, were practitioners before the dawn of the internet.* (Director-9)

Many participants shared their view that cyber expertise is needed for boards to effectively monitor cyber risk. For example, one executive explained that expertise is needed to prevent check-the-box oversight:

> *[Cybersecurity] is one of those areas where there needs to be time, energy and expertise. And you need to have the right makeup of the board to make sure that it's not just a pencil to check the box. … You need to have at least one, if not a couple, people that can really challenge [executives] and ask all the right questions… You want to have people on the board that really have domain expertise in there. That they can look at the CEO and say, you're doing a good job or, in some cases, you're weak in this area. …[T]his is an area where every board, with any company of scale, should have this kind of expertise.* (Executive-8)

In contrast, some participants discounted the importance of directors having cyber expertise per se. For example, some directors claimed that general business experience sufficiently qualified them to oversee cybersecurity:

> *[O]n my boards, I think 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*. (Director-3)

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

> *[S]ometimes, people with the least technical knowledge in many ways have a better perspective on understanding business risk and enterprise risk associated with it, but they're thinking about it in [a] holistic context than dropping you down into this technical silo, which you're not an expert in anyway. The issue is broader than that. … I think it's a topic that everybody can contribute to, and maybe contribute differently. It's important to think about the totality of the risk and the problem.* (Director-6)

Interestingly, whereas most CISOs argued that board membership should have cybersecurity expertise, some CISOs believed that board-level cybersecurity expertise is unnecessary or can even be detrimental to the cybersecurity function in some cases. For example, one CISO thought that a director with cybersecurity expertise could interfere with or unhelpfully divert the management of cybersecurity:

> *There's a little bit of risk that they could want to get their fingers into things a little bit more than they probably should as part of being a board member. … Certain things a board member can say or ask for can really spin off an organization into going down a path of doing a lot of work that may not ultimately have a lot of value to it.* (Executive-3)

Another way that cybersecurity expertise can be counterproductive is if it decreases the frequency of board–CISO interactions:

> *It used to be when the chair of the audit and risk committee would have a particular question, she'd call me and I'd tell her whatever. Now, she always wants [to talk to the new board member with cybersecurity expertise]. And it's like, fine. I don't care, [that person] and I get along fine. In fact, we probably agree on a lot. But again, I think to some degree, it may have hampered some conversation.* (Executive-6)

Others felt that the mere presence of a director with cybersecurity expertise on the board could cause the rest of the board to over-rely on that person (Director-3) or create a false sense of security among the board in general:

> *I think if you're not careful, you've created a false sense of security—an illusion that you now have this "expert" that has such a breadth of knowledge that you're*

> *going to be able to manage this differently. I honestly don't think that's very possible.* (Director-6)

Some participants shared practical barriers that prevent boards from having directors with cybersecurity skills. For example, despite the desirability or even the need for board expertise, participants cite the scarcity of such qualifications in the director labor pool as preventing boards from achieving the desired levels of cybersecurity expertise (Consultant-5). Others felt that it is "not reasonable" for board members to have a detailed understanding of cybersecurity because "that's the job of the CISO and the [cybersecurity] team" (Consultant-4) and that investment would be better spent on cybersecurity staff working at the company (Director-4).

Participants also clarified that cybersecurity cannot be a board member's sole area of expertise because of the responsibility of board members to oversee the business generally:

> *[Y]ou really want people [on the board] that are very broad-based in knowledge and not necessarily [have] deep expertise. … [H]aving board members that are much broader and can contribute more broadly may be more beneficial … [compared to] directors [with] more narrow technology experience.* (Executive-6)

> *To give up a board seat to a single-skill director can have different impacts on that board. They would rather have somebody with broader business experience so they can hit topics across all the organization.* (Consultant-2)

These statements illustrate a perception that a director with cybersecurity expertise will have little to contribute to the board beyond cybersecurity (Consultant-7), and companies should not "waste the board seat on just someone who goes with their top technology, not understanding or helping drive their business strategy" (Director-5). Rather than appointing a director with only narrow cybersecurity skills to bring to the table, some participants suggested that an independent consultant can be engaged to support the board without giving up a board seat:

> *I don't think you should get a board member that the only thing he or she brings to the board is cybersecurity. If that's all you want, then don't get a board member. Just go hire an outside consultant and have them come and do that every time. Because a board member has a lot of other things that he or she has got to worry*

> *about besides cybersecurity. … Because you can buy that. You can buy that.* (Director-1)

However, other participants raised concerns about relying on outsourced expertise rather than having a board-level cyber expert. First, relying on consultants when the board does not have cybersecurity expertise can result in the complete outsourcing of oversight, consistent with self-efficacy theory. Second, the board may not be able to determine what types of cybersecurity engagements are needed. In fact, consultants must often explain to boards the different types of cybersecurity-related engagements that are available (Consultant-3). Third, directors may not be able to assess the quality of a consulting firm's work product (Consultant-6). When asked whether directors have the ability to assess the quality of consultants' work, one consultant responded:

> *No, I think they can't. I think frequently they'll turn to a well-known name, usually an audit company—KPMG or Deloitte or somebody. They'll turn to either their internal audit company or their external company. And frequently, those companies will throw in a cyber audit or a cyber review as a freebie. "Oh, sure, we are an external audit company, and we can do that for you, and it won't cost you anything," or "it'll cost you very little." And I mean, you get what you pay for. … [Y]ou're literally going to get the same report they did for their last client. It's a complete template, complete cookie cutter. And we've even seen times when they've failed to take the name of the last client off the PowerPoint slides. (Consultant-3)*

Given the abovementioned benefits of expertise on oversight effectiveness, some nomination committees have added cybersecurity expertise or skill as a key factor for recent or upcoming appointments (Director-5, Executive-8). Table 6 presents additional examples of evidence of participant perspectives on the need for directors to have this expertise. However, an open question remains of what actually qualifies as cybersecurity expertise, which we consider next.

What Qualifies as Relevant Expertise

Given the predominantly held view that cybersecurity expertise is beneficial and thus needed at the board level, an important question is what qualifies a director as having cybersecurity "expertise." Although participants acknowledged that training programs aimed at board members

are helpful, such as the NACD's "Cyber-Risk Oversight Certificate" program for directors (NACD 2021), they stressed that such programs are not substitutes for work experience in cybersecurity (Executive-8). Participants characterized the ideal board member with cybersecurity expertise as someone who has experience in managing cybersecurity (such as a CISO) or who has directly overseen cybersecurity (such as a CIO or CTO):

> *[W]hat makes a good board member relative to cybersecurity, in an ideal world? They're a former CISO. They have sat in the chair, they've done it before, they've done it well, they know what "good" looks like. I think that's what makes any board member a good board member is they know what excellence [is]… …and they can hold the company to a higher standard by governing it accordingly. That's in an ideal world.*
>
> *In a subpar, sub-ideal world, it may be somebody who, at least, was in a related field, maybe somebody who was in a technology company, maybe an educator who teaches cybersecurity, or at least he knows the frameworks and the questions to ask.* (Consultant-7)

Actual expertise in cybersecurity is more important than a particular job title, with participants acknowledging that some CIOs are very proficient in cybersecurity and others are not. For example, in some organizations, the cybersecurity function may be independent from the IT function and the CIO (Executive-3, Executive-6). Others were careful to point out that technology expertise is not the same as cybersecurity expertise, "Just like running a factory is not the same as building a factory" (Director-2). One CTO and former director admitted:

> *[Is there] a proclivity for technologists like myself to overestimate our cyber skills? Yes. I think that's fair. Cyber is its own discipline. It's just its own knowledge base. If you're building things, there is a set of considerations and if you're securing things, it's a different [set]. … It's such a different mindset and a different set of tools."* (Director-9)

Participants argued that "you have to have subject matter expertise from past experience [for a director's expertise] to be relevant" (Consultant-3) and that it is "important for boards to have people that have actually got their hands dirty" working in cybersecurity (Executive-8). Similarly,

participants commented that experience in board oversight of cybersecurity—even in a specialized committee, such as audit or risk—is insufficient to qualify a director as a cybersecurity expert:

> *You can't just say, "I served on a committee," that's not enough. (Unless you served on a committee maybe at a technology company for 10 years. I mean that might be different.) You need to get somebody on the board who has a more technical background, who's been a CIO or had to be in these kinds of [cybersecurity-related] environments.* (Director-11)

However, a complicating issue for characterizing expertise based on past work experience is that cybersecurity expertise decays, so that a director with prior CISO work experience may not necessarily be current in their cybersecurity skills (Consultant-2, Director-9). Table 7 presents additional selections of interview evidence of participant perspectives on what qualifies as cybersecurity expertise.

V. CONCLUSION

Our qualitative field study incorporates perspectives from board directors, cybersecurity executives, and cybersecurity consultants who support boards to investigate how boards conduct cybersecurity oversight and the influence of boards' cybersecurity expertise. Our interviews suggest that the level of expertise has a pervasive impact on the attention boards give to cybersecurity issues and the quality of their oversight. Our participants revealed that a lack of expertise can result in superficial oversight with a compliance orientation, which is inconsistent with regulators' and investors' expectations for the board to provide substantive oversight of cybersecurity. Our findings also suggest that boards are often unable to ask effective questions, understand the answers they receive, or detect filtered or withheld reporting. More broadly, the expertise gap between boards and the cybersecurity executives they oversee can result in circular governance, a dynamic whereby executives coach the board not only on basic cybersecurity principles but also on the process of oversight itself. Such circular governance appears to strongly

contradict expectations from agency theory that boards will provide independent oversight of management, and is more consistent with low expertise resulting in directors ceding control of oversight, as predicted by self-efficacy theory. Overall, our findings highlight that without sufficient domain-specific expertise, the board is unlikely to fulfill the monitoring role emphasized in the agency-based perspective of corporate governance.

Our results have implications for the ongoing debate on whether cybersecurity expertise is needed at the board level and whether/how board cybersecurity expertise should be required for public firms (S.808 2021). Although our evidence suggests that effective oversight requires domain expertise and raises the potential for cybersecurity-related corporate governance failures when inexpert boards cede control of oversight, we are careful to note that the policy implications of our findings are not obvious. More broadly, our study does not encompass a full examination of the relative benefits of cybersecurity expertise vis-à-vis other director qualifications. Thus, while we do not attempt to directly investigate the costs and benefits of requiring cybersecurity expertise at the board level, we believe that our study provides useful insights for policymakers and shareholders as they make decisions relative to board qualifications.

We also contribute to the literature on the role of director expertise in determining oversight effectiveness. Given that cybersecurity risk oversight is often delegated to audit committees, our findings add to our understanding of what audit committee characteristics enhance its effectiveness. While audit committee duties typically include the oversight of financial reporting and enterprise risk management, most extant research focuses on financial reporting (e.g., Klein 2002; Gendron and Bédard 2006; Cohen et al. 2014; Lisic et al. 2019; Couchoux 2021). In contrast, less is known about what characteristics are important for risk oversight, particularly for cybersecurity risk. Our study responds to the call to investigate how cybersecurity risk is handled

as part of a firm's enterprise risk management (Cohen, Krishnamoorthy, and Wright 2017) and highlights that cybersecurity is normally outside the expertise of most directors, yet boards are still tasked with overseeing the increasingly prominent risks in this very technical domain. Our findings suggest that boards often lack the necessary expertise to fulfill the risk oversight role expected of them.

A related concern is that the audit committees may be overburdened with both financial reporting and risk oversight responsibilities (KPMG 2015). For example, when audit committees are tasked with risk-related oversight responsibilities in addition to their primary focus on financial reporting, the quality of the latter may suffer (Ashraf, Choudhary, and Jaggi 2021). Couchoux (2021) explores audit committee styles and finds that, when audit committees are burdened with disparate tasks, their expertise is unlikely to relate to all of the committee's tasks. To the extent that financial reporting and general risk oversight represent competing demands on director attention, our findings suggest that, in the absence of cybersecurity expertise, boards may give inadequate attention to cybersecurity risks, calling into question the appropriateness of tasking the audit committee with risk oversight duties.

Although the focus of this study is on cybersecurity, we expect that our findings have relevance to other areas that boards are asked to oversee, despite not having relevant experience or expertise in those areas. For example, boards are increasingly expected to oversee culture, diversity, and inclusiveness, as well as environmental initiatives (Vittorio 2019; Burke 2021), despite the fact that skills in these areas may be unrelated to the skills underlying the directors' nominations to the board in the first place. Although the extant archival evidence finds that expertise in various domains is associated with firm outcomes, through the lens of self-efficacy theory, our study provides a rich description of *how* expertise affects the oversight process.

References

Abbott, L. J., S. Parker, and G. F. Peters. 2004. Audit committee characteristics and restatements. *AUDITING: A Journal of Practice & Theory* 23 (1): 69-87.

Agarwal, R., V. Sambamurthy, and R. M. Stair. 2000. The evolving relationship between general and specific computer self-efficacy: An empirical assessment. *Information Systems Research* 11 (4): 418.

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

Aguilar, L. A. 2014. *Boards of directors, corporate governance and cyber-risks: Sharpening the focus*. New York Stock Exchange, (June 10, 2014). Available at: https://www.sec.gov/news/speech/2014-spch061014laa#_edn26 (last accessed July 22, 2020).

Amir, E., S. Levi, and T. Livne. 2018. Do firms underreport information on cyber-attacks? Evidence from capital markets. *Review of Accounting Studies* 23 (3): 1177-1206.

Ashraf, M. 2021. The role of peer events in corporate governance: Evidence from data breaches. *The Accounting Review*.

Ashraf, M., P. Choudhary, and J. Jaggi. 2021. Audit committee oversight and financial reporting reliability: Are audit committees overloaded? Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3433389.

Bandura, A. 1977. Self-efficacy: Toward a unifying theory of behavioral change. *Psychological Review* 84 (2): 191-215.

———. 1982. Self-efficacy mechanism in human agency. *American Psychologist* 37 (2): 122-147.

———. 1986. The explanatory and predictive scope of self-efficacy theory. *Journal of Social and Clinical Psychology* 4 (3): 359-373.

———. 1997. *Self-efficacy: The exercise of control*. New York: W.H. Freeman.

———. 2001. Social cognitive theory: An agentic perspective. *Annual Review of Psychology* 52 (1): 1.

Banker, R. D., and C. Feng. 2019. The impact of information security breach incidents on CIO turnover. *Journal of Information Systems* 33 (3): 309-329.

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

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

Beasley, M. S., J. V. Carcello, D. R. Hermanson, and T. L. Neal. 2009. The audit committee oversight process. *Contemporary Accounting Research* 26 (1): 65-122.

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

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

Blosfield, E. 2021. Maine one of latest states to enact NAIC-inspired Insurance Data Security Act. In *Insurance Journal*.

Bonner, S. E., and B. L. Lewis. 1990. Determinants of auditor expertise. *Journal of Accounting Research* 28: 1-20.

Bouffard-Bouchard, T. 1990. Influence of self-efficacy on performance in a cognitive task. *The journal of social Psychology* 130 (3): 353-363.

Burke, J. J. 2021. Do boards take environmental, social, and governance issues seriously? Evidence from media coverage and CEO dismissals. *Journal of Business Ethics* (forthcoming).

Cervone, D., and P. K. Peake. 1986. Anchoring, efficacy, and action: The influence of judgmental heuristics on self-efficacy judgments and behavior. *Journal of Personality and Social Psychology* 50 (3): 492-501.

Chen, X., Q. Cheng, and X. Wang. 2015. Does increased board independence reduce earnings management? Evidence from recent regulatory reforms. *Review of Accounting Studies* 20 (2): 899-933.
Cheng, J. Y.-J., B. Groysberg, P. Healy, and R. Vijayaraghavan. 2021. Directors' perceptions of board effectiveness and internal operations. *Management Science* 67 (10): 6399-6420.
Cohen, J. 1960. A coefficient of agreement for nominal scales. *Educational and Psychological Measurement* 20 (1): 37-46.
Cohen, J., G. Krishnamoorthy, and A. Wright. 2017. Enterprise risk management and the financial reporting process: The experiences of audit committee members, CFOs, and external auditors. *Contemporary Accounting Research* 34 (2): 1178-1209.
Cohen, J. R., U. Hoitash, G. Krishnamoorthy, and A. M. Wright. 2014. The effect of audit committee industry expertise on monitoring the financial reporting process. *The Accounting Review* 89 (1): 243-273.
Compeau, D. R., and C. A. Higgins. 1995. Computer self-efficacy: Development of a measure and initial test. *MIS Quarterly* 19 (2): 189-211.
Couchoux, O. 2021. Audit committee members' style of oversight: Juggling expertise and complexity. *Working Paper*.
Council of Institutional Investors (CII). 2016. Prioritizing cybersecurity: Council of Institutional Investors.
Cybersecurity Disclosure Act of 2021.
DeFond, M. L., R. N. Hann, and H. U. Xuesong. 2005. Does the market value financial expertise on audit committees of boards of directors? *Journal of Accounting Research* 43 (2): 153-193.
Doan, M. 2019. Companies need to rethink what cybersecurity leadership is: Harvard Business Review.
Dodgson, M. K., C. P. Agoglia, G. B. Bennett, and J. R. Cohen. 2020. Managing the auditor-client relationship through partner rotations: The experiences of audit firm partners. *The Accounting Review* 95 (2): 89-111.
Dowling, C. 2009. Appropriate audit support system use: The influence of auditor, audit team, and firm factors. *The Accounting Review* 84 (3): 771-810.
Eisenhardt, K. M. 1989. Agency theory: An assessment and review. *Academy of Management Review* 14 (1): 57-74.
EY. 2020. What companies are disclosing about cybersecurity risk and oversight, edited by Ernst & Young.
Faleye, O., R. Hoitash, and U. Hoitash. 2011. The costs of intense board monitoring. *Journal of Financial Economics* 101 (1): 160-181.
Fama, E. F. 1980. Agency problems and the theory of the firm. *Journal of Political Economy* 88 (2): 288-307.
Fama, E. F., and M. C. Jensen. 1983. Separation of ownership and control. *Journal of Law and Economics* 26 (2): 301-325.
Federal Trade Commission (FTC). 2019. Standards for Safeguarding Customer Information.
———. 2021. Corporate boards: Don't underestimate your role in data security oversight, edited by J. Ho. Washington, D.C.
Ferracone. 2019. *Good governance: Do boards need cyber security experts?* Forbes. Available at: https://www.forbes.com/sites/robinferracone/2019/07/09/good-governance-do-boards-need-cyber-security-experts/?sh=15d506f21859 (last accessed October 5, 2021).
Fich, E. M., and A. Shivdasani. 2007. Financial fraud, director reputation, and shareholder wealth. *Journal of Financial Economics* 86 (2): 306-336.
Field, L., M. Lowry, and A. Mkrtchyan. 2013. Are busy boards detrimental? *Journal of Financial Economics* 109 (1): 63-82.
Fisher, R. J. 1993. Social desirability bias and the validity of indirect questioning. *Journal of Consumer Research* 20 (2): 303-315.
Fox, J. 2021. Cybersecurity Statistics for 2021: Cobalt Labs, Inc.
Free, C., A. J. Trotman, and K. T. Trotman. 2021. How Audit Committee Chairs Address Information-Processing Barriers. *Accounting Review* 96 (1): 147-169.

Gartner. 2021. Forecast: Information security and risk management, worldwide, 2019-2025, 1Q21 update.
Gendron, Y., and J. Bédard. 2006. On the constitution of audit committee effectiveness. *Accounting, Organizations and Society* 31 (3): 211-239.
Gist, M. E. 1987. Self-efficacy: Implications for organizational behavior and human resource management. *Academy of Management Review* 12 (3): 472-485.
Goh, B. W. 2009. Audit committees, boards of directors, and remediation of material weaknesses in internal control. *Contemporary Accounting Research* 26 (2): 549-579.
Hambrick, D. C., V. F. Misangyi, and C. A. Park. 2015. The quad model for identifying a corporate director's potential for effective monitoring: Toward a new theory of board sufficiency. *Academy of Management Review* 40 (3): 323-344.
Hayne, C., and M. Vance. 2019. Information intermediary or de facto standard setter? Field evidence on the indirect and direct influence of proxy advisors. *Journal of Accounting Research* 57 (4): 969-1011.
Hillman, A. J., and T. Dalziel. 2003. Boards of directors and firm performance: Integrating agency and resource dependence perspectives. *Academy of Management Review* 28 (3): 383-396.
Hoitash, U., R. Hoitash, and J. C. Bedard. 2009. Corporate governance and internal control over financial reporting: A comparison of regulatory regimes. *The Accounting Review* 84 (3): 839-867.
Huang, H. H., and C. Wang. 2021. Do banks price firms' data breaches? *The Accounting Review* 96 (3): 261-286.
Institute of Internal Auditors (IIA). 2010. Global technology audit guide (GTAG(R)) 15 information security guidance, edited by P. Love, J. Reinhard, A. J. Schwab and G. Spafford. Altamonte Springs, FL: Institute of Internal Auditors.
Internet Security Alliance (ISA), and National Association of Corporate Directors (NACD). 2020. Internet Security Alliance and National Association of Corporate Directors Release New Guide for Cyber-Risk Oversight. Arlington, VA: Internet Security Alliance.
Iskandar, T. M., R. N. Sari, Z. Mohd-Sanusi, and R. Anugerah. 2012. Enhancing auditors' performance: The importance of motivational factors and the mediation effect of effort. *Managerial Auditing Journal* 27 (5): 462-476.
Jackson, R. J. 2018. Speech: Corporate governance: On the front lines of America's cyber war, edited by Securities and Exchange Commission.
Jensen, M. C. 1993. The modern industrial revolution, exit, and the failure of internal control systems. *Journal of Finance* 48 (3): 831-880.
Jensen, M. C., and W. H. Meckling. 1976. Theory of the firm: Managerial behavior, agency costs and ownership structure. *Journal of Financial Economics* 3 (4): 305-360.
Kamiya, S., J.-K. Kang, J. Kim, A. Milidonis, and R. M. Stulz. 2021. Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics* 139 (3): 719-749.
Klein, A. 2002. Audit committee, board of director characteristics, and earnings management. *Journal of Accounting and Economics* 33 (3): 375-400.
KPMG. 2015. Audit committees cite uncertainty, volatility and high risk environment as top challenges In 2015. In *More Boards Reallocating Oversight Duties as Risk Environment Strains Audit Committee Agendas*: KPMG LLP.
———. 2021. Views from the boardroom: 2021 pulse survey.
Krishnan, J. 2005. Audit committee quality and internal control: An empirical analysis. *The Accounting Review* 80 (2): 649-675.
Larcker, D. F., P. C. Reiss, and B. Tayan. 2017. Critical update needed: Cybersecurity expertise in the boardroom. *Rock Center for Corporate Governance at Stanford University Closer Look Series: Topics, Issues and Controversies in Corporate Governance No. CGRP-69*: 17-70.
Lisic, L. L., L. A. Myers, T. A. Seidel, and J. Zhou. 2019. Does audit committee accounting expertise help to promote audit quality? Evidence from auditor reporting of internal control weaknesses. *Contemporary Accounting Research* 36 (4): 2521-2553.

Maddux, J. E., and E. M. Kleiman. 2020. Self-efficacy: The power of believing you can. In *The Oxford Handbook of Positive Psychology*, edited by C. R. Snyder, S. J. Lopez, L. M. Edwards and S. C. Marques: Oxford University Press.
Malsch, B., and S. E. Salterio. 2016. "Doing good field research": Assessing the quality of audit field research. *AUDITING: A Journal of Practice & Theory* 35 (1): 1-22.
McDaniel, L., R. D. Martin, and L. A. Maines. 2002. Evaluating financial reporting quality: The effects of financial expertise vs. financial literacy. *The Accounting Review* 77 (s-1): 139-167.
Miles, M. B., A. M. Huberman, and J. Saldaña. 2020. *Qualitative Data Analysis: A Methods Sourcebook*. 4th Edition ed. Thousand Oaks, CA: Sage Publications.
Morgan, S. 2019. Global cybersecurity spending predicted to exceed $1 trillion form 2017-2021. *Cybercrime Magazine*.
Morse, J. M. 1995. The significance of saturation. *Qualitative Health Research* 5 (2): 147-149.
Myers, M. D. 2009. *Qualitative Research in Business & Management*. Thousand Oaks, CA Sage Publications Ltd.
National Association of Corporate Directors (NACD). 2018. 2018-2019 NACD Public Company Governance Survey. Arlington, VA: NACD.
———. 2020. Cyber-risk oversight 2020: Key principles and practical guidance for corporate boards, edited by National Association of Corporate Directors (NACD) and Internet Security Alliance.
———. 2021. *Cyber-Risk Oversight Certificate*. Available at: https://www.nacdonline.org/events/detail.cfm?ItemNumber=37092 (last accessed May 25, 2021).
New York Department of Financial Services. 2017. Cybersecurity requirements for financial services companies. In *23 NYCRR s 500.4(b)*.
Paternoster, R., and S. Simpson. 1996. Sanction threats and appeals to morality: Testing a rational choice model of corporate crime. *Law and Society Review* 30 (3): 549-583.
PCAOB. 2018. Panel discussion: Cybersecurity. In *Standing Advisory Group Meeting*, edited by Public Company Accounting Oversight Board. Washington, DC: PCAOB.
Piquero, A. R., J. A. Bouffard, N. L. Piquero, and J. M. Craig. 2016. Does morality condition the deterrent effect of perceived certainty among incarcerated felons? *Crime & Delinquency* 62 (1): 3-25.
PwC. 2019. PwC's 2019 Annual Corporate Directors Survey, edited by PwC Governance Insights Center.
———. 2021. Stronger enforcement puts teeth in cyber and privacy rules.
Saldaña, J. 2013. *The Coding Manual for Qualitative Researchers*. Second ed: Sage Publications.
SEC. 2003. Final Rule: Disclosure required by Sections 406 and 407 of the Sarbanes-Oxley Act of 2002. In *Release Nos. 33-8177; 34-7235*, edited by Securities and Exchange Commission. Washington, D.C.: SEC.
———. 2009. Regulation S-K, edited by Securities and Exchange Commission. Washington D.C.
———. 2011. Cybersecurity. In *SEC Division of Corporation Finance*, edited by Securities and Exchange Commission. Washington D.C.: SEC.
———. 2018. Commission Statement and Guidance on Public Company Cybersecurity Disclosures, edited by Securities and Exchange Commission. Washington, D.C.: SEC.
———. 2021a. Cybersecurity Risk Governance, edited by Securities and Exchange Commission. Washington, D.C.
———. 2021b. SEC announces three actions charging deficient cybersecurity procedures. In *2021-169*. Washington, D.C.: Securities and Exchange Commission.
———. 2021c. SEC charges issuer with cybersecurity disclosure controls failures. In *2021-102*. Washington, D.C.: Securities and Exchange Commission.
———. 2021d. SEC charges Pearson Plc for misleading investors about cyber breach. In *2021-154*. Washington, D.C.: Securities and Exchange Commission.
Tidy, J. 2021. U.S. companies hit by 'colossal' cyberattack. In *BBC News*: BBC.
Tunggal, A. T. 2021. Why is cybersecurity important. In *Cybersecurity*: Upguard.
Sarbanes-Oxley Act of 2002. 107-204. July 30.

U.S. Department of the Treasury. 2001. Interagency Guidelines Establishing Standards for Safeguarding Customer Information and Recision of Year 2000 Standards for Safety and Soundness, edited by Department of the Treasury.

———. 2020. Consent Order In *AA-EC-20-49*, edited by Department of the Treasury. Washington, D.C.: U.S. Department of the Treasury, Office of the Comptroller of the Currency.

Vittorio, A. 2019. Diversity, culture among corporate boards' top trends in 2019. *Bloomberg Law*, January 2, 2019.

Weisbach, M. S. 1988. Outside directors and CEO turnover. *Journal of Financial Economics* 20: 431-460.

Xie, B., W. N. Davidson, and P. J. DaDalt. 2003. Earnings management and corporate governance: The role of the board and the audit committee. *Journal of Corporate Finance* 9 (3): 295-316.

Xu, H., H.-H. Teo, B. C. Y. Tan, and R. Agarwal. 2012. Research note—Effects of individual self-protection, industry self-regulation, and government regulation on privacy concerns: A study of location-based services. *Information Systems Research* 23 (4): 1342-1363.

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

Yoo, C. W., J. Goo, and H. R. Rao. 2020. Is cybersecurity a team sport? A multilevel examination of workgroup information security effectiveness. *MIS Quarterly* 44 (2): 907-931.

Table 1 Summary of Theoretical Lenses

Theoretical Lenses	
Agency theory	**Description:** Shareholders hire managers as their agents to operate the firm, including managing investments, profitability, and related downside risks. Managers are self-interested and have motives distinct from shareholders that cannot be costlessly resolved through contracting. The board of directors represents shareholders and one of their primary functions is to constrain management opportunism through providing oversight (Fama and Jensen 1983). **Role of expertise:** By assumption, the board has sufficient expertise fulfill their oversight role (Fama and Jensen 1983; Jensen 1993). **Expected findings:** The board recognizes the potential for agency conflicts with management and provides substantive, independent oversight of the firm's cybersecurity program.
Self-efficacy theory	**Description:** Self-efficacy is an individual's perception of their domain-specific capabilities to act upon prospective situations due to past experience and performance (Bandura 1982, 1986). **Role of Expertise:** Expertise increases an individual's self-efficacy (Bandura 1986), which in turn drives an individual's focus and actions, and leads to higher attention and improved performance. **Expected findings:** In the absence of cybersecurity expertise, boards will limit attention to cybersecurity issues. With low cybersecurity expertise, directors are more likely to cede oversight control to internal and external experts.

Table 2 Interview Details

Panel A: Director interview details

Interview #	Committee participation related to cybersecurity oversight	# of director positions	Interview length (minutes)	Cyber Expertise	Declared skill on proxy statement	Market Cap	Represented industries
Director-1	Audit (chair)	3	53	Low	No	Mid	Wholesale trade Retail trade Services
Director-2	Audit (member)	4	50	Med	Yes	Large	Manufacturing Wholesale trade
Director-3	Audit (chair)	2	67	Low	No	Mid	Financial services Manufacturing
Director-4	Audit (member)	2	63	Med	Yes	Mid	Services
Director-5	Audit (member)	2	49	High	NA	Mid	Services
Director-6	Audit (chair, member)	3	62	Med	Yes	Large	Construction Financial services
Director-7	None	3	63	Low	No	Mid	Manufacturing Retail trade Financial services
Director-8	Audit (member)	1	55	Low	No	Mid	Services
Director-9	None	1	32	High	NA	Mid	Services
Director-10	Audit (member), Risk (member)	6	43	Low	No	Mid	Services Financial services
Director-11	Audit (member)	7	32	High	No	Mid	Services Financial services

Panel B: Executive interview details

Interview #	Position	Interview length (minutes)	Cyber Expertise	Market Cap	Represented industries
Executive-1	CIO	52	High	Mid	Wholesale trade
Executive-2	CISO	66	High	Mid	Services
Executive-3	CISO	60	High	Mid	Financial services
Executive-4	CISO	46	High	Large	Transportation & Public Utilities
Executive-5	CISO	61	High	Mid	Services
Executive-6	CISO	63	High	Large	Financial services
Executive-7	CISO	63	High	Large	Manufacturing Services
Executive-8	CSO	63	High	Large	Manufacturing
Executive-9	CISO	54	High	Large	Wholesale trade

Panel C: Consultant interview details

Interview #	Interview length (minutes)	Cyber Expertise	Type of consulting firm
Consultant-1	45	High	Technology solutions firm
Consultant-2	50	Medium	Big-4 accounting firm
Consultant-3	53	High	Cybersecurity consulting firm
Consultant-4	48	High	Cybersecurity risk ratings firm
Consultant-5	80	High	Risk management consulting firm
Consultant-6	84	High	Risk management consulting firm
Consultant-7	67	High	Big-4 accounting firm

This table provides information about our three categories of interviewees and the firms they represent. Panel A presents director participants. The number of director positions reflects corporate director positions within five years of their interviews. Cybersecurity expertise is based on their self-disclosure and verification based on their work history. Director-5 and Director-9 hold positions on private company boards and therefore no proxy statements were available. With the exception of Director-9 who was an executive director, all directors were independent directors. Two researchers independently categorized each participant and reconciled any differences in categorization. Market capitalization ranges are: Mid-cap, $2-9.9 billion; Large-cap, $10+ billion. This is based on the director's largest firm, if publicly listed, or annual revenues, if a private firm.

Table 3 Additional Interview Evidence of How Expertise Affects Boards' Cybersecurity Oversight

4.1.1 The influence of expertise on attention
[B]oard members want to be useful. They want to make the company successful and therefore, they are inclined to speak more about it and dwell on things where they feel like they can contribute. (Director-9) Yeah, because your general board members, because they have their day life and whatever is exacting or commanding their attention in the course of any given week, may not have time to dabble in paradigm battles… And to even be positioned to even have the thought or to have it occur to you to even raise the implications of these emergent technologies, is probably not something a board member whose principal interests lie elsewhere, would have had the time to have even become aware that there's a question out there that you might want to pose or ask. (Executive-7) [T]he board should make sure it's got its governance structure right…. And if they do get that right, it has real world effects. Because then there's somebody on the board who is knowledgeable about cyber, and that means that the CISO has somebody to talk to. And there should be a line of communication between that board member and the CISO. And usually, that also means that the CISO gets out from under the CIO, doesn't report to the CIO directly. So if you get the governance model right, these issues are going to get better funding and then get more time and attention. (Consultant-3)
4.1.2 How expertise influences the quality of questions asked
But [X, a director with more cyber expertise] just comes up with good ideas, good things to think about, or for management to think about. Not only just where do the ones and zeros go, but how are you structured, your organization? Where are you spending your time in your organization in your information areas? You know, your data processing areas and stuff. (Director-1) I spend a lot of time in this area, so I will always make sure that I'm comfortable personally, and then I'll meet with the CISO if we have a cyber security discussion, I'm probably asking 3 or 4 questions for every 1 question that somebody else asks. Because I spend more time on it and I'm also trained on it, so I think I know better what to ask. (Director-2) [Director X] is probably our most versed person in his experience with these kinds of issues…. I know I wasn't brought in because of my cybersecurity expertise…. It's helpful to have someone who's kind of lived in the world on the front edge of things a little bit, and I think boards certainly would benefit by having somebody that has knowledge of what are the questions that need to be asked and the issues that need to be addressed so that you don't just get a kind of a glossy eye, 'we're on top of this and let us show you all the insurance we have to protect against all these different possibilities….' He just might ask more questions and have more insights than the average board member would... he tends to be someone who brings a little bit more to the party for that. (Director-8)
4.1.3 Expertise influences how answers are received
[In response to: Did they ask you any follow-up questions?] Nope. Which shows the maturity level of the board. They wouldn't be able to ask questions. (Executive-5) There's a language barrier here. Boards don't want to be embarrassed. They don't want to sit in a room and say, "What is that acronym," and, "What does that mean?" They're not going to do that. (Consultant-6) That doesn't mean that they understand the answers, and that doesn't mean that they know what to do about it… So boards are getting smarter and smart enough to ask the questions. They're just not yet smart enough to interpret what the CISO is saying. (Consultant-7)

Table 4 Participant-provided Examples of Questions Directors Ask

Superficial	• Do we know what our critical assets are? (Executive-4) • Hey, what are we doing for cybersecurity? (Executive-2, Director-11) • Explain this whole cybersecurity thing to me. (Consultant-7) • How are we doing? (Consultant-3) • Are we moving in the right direction or not, and what are we doing about it if we're not? (Executive-1) • Are we compliant? (Consultant-1) • Do you have somebody in charge of it?. . . Do they know what they're doing? (Executive-2) • Do we have that risk? Or, could that have happened to us? [regarding hack in media] (Director-3, Director-5) • What's our exposure to ransomware? (Consultant-4) • Do you have the right resources to fix it? (Executive-1) • Okay, what are we going to do about these things? (Director-1) • What's our disaster recovery plan for a cyber emergency look like? (Consultant-3) • This is great. What does that mean to us, from a business perspective? (Consultant-7) • Why haven't you [done penetration tests]? When will you be doing it, and when will you be telling me the results? (Director-3)
Substantive	• Knowing our critical assets are X. . . should we be changing our security model in these areas? (Executive-4) • How are you structured, your organization? Where are you spending your time in your organization in your information areas? You know, your data processing areas and stuff. (Director-1) • Hey, what's going on here? I thought we concluded we were going to do this. How do we get this back on track? (Director-1) • What sort of CASB do we have, and is it good enough? (Consultant-3) • Are you funded? How are you handling the cyber talent shortage? Do you get the right support? What's the tone? (Executive-6) • To what extent has our team embraced the solutions that are now proactively preventing malware and ransomware two years in advance of their appearance? (Executive-7) • How well insured are we? Which policies relate to this, for how much money? What are the requirements of those policies? Are we meeting the requirements of those policies? Can we demonstrate that we did that when we have a cyber breach, and now we want to make a claim? (Consultant-6) • What is our policy on notification to law enforcement? When are we going to do it, on what? Who has the authority to do it? How does it work? What are the risks? (Consultant-6) • Do we encrypt our source code? Do we actually carry PII in un-encrypted form? Are we PCI compliant on our credit card transactions? Do we actually throttle the database such that you cannot pull all customer records at one time? (Director-11)

Table 5 Additional Interview Evidence of the Relationship Between the Board and the CISO

4.2.1 Lack of expertise requires coaching by CISOs	
Educating the board	The last presentation was to the full board, and they were just generally asking questions. A lot of them were generally asking questions about more, just trying to seek better understanding around cyber and what have you.... For a lot of the individuals, they were trying to still learn about cybersecurity. There were times where, especially right now with the ... different types of cyberattacks that are occurring, there's a certain level of interest to really understanding more. (Executive-3) One of the things that we implemented the first year I was here is a discipline, or I should say, a cadence where, at least once a year, we have a board education session. One year it was just security 101 kind of stuff. The anatomy of a program, how it's built, how you evolved to the strategy, how you execute, that kind of stuff. And then we did a tabletop demonstration, how we do our annual cybersecurity, executive tabletop exercises. We had one session on, 'How do you protect yourself from the criminal?' kind of thing. So every year we have that, and that's really helped in board education. (Executive-6) [T]he executive committee is essentially attending the audit committee meeting that I update in, which is great for me because it's a super opportunity not just to educate the board but [also] the executive committee and keep them in the loop." (Executive-9)
Conditioning the board	But we have really hammered that home, and this is the five functions that you align a cybersecurity program to. And this is the framework we're using to manage cybersecurity. So this is what one should look like, these are the things that you should have in place. And then we go through a process saying, "Well, this is the maturity of us against that framework of how we've implemented it." And then the rest of it becomes a little bit of trying to understand what's the best way to help them provide oversight, what are the best kind of reports. (Executive-3) [L]et us [the CISO and their team] tell you what the risks are, let us tell you what we're most concerned about, and for those things we're concerned about we're going to report back to you on the progress we make on remediating that, and then... let me show you how we're protected from an insurance standpoint, too, so if something does go bump in the night, it's not going to harm the company's financial situation. (Director-8) I took one of those [articles], "The Top 10 Questions Boards Should Ask CISOs." We took the questions, I filled it out, and then we just gave it to the board members and their repository to pre-answer before they ask. (Executive-6)
4.2.2 Expertise enables board members to detect false or withheld information	
	There is always a bit of "protect your house." We know that information is filtered to the board and that's why it's important to get outside sources of information…. [Regarding whether the filtering is unique to cybersecurity] I think it becomes more challenging because the boards may not know enough to ask as many questions. If you have a cyber expert it is probably not as big of an issue. It is more challenging because of the nature of it. …IT is a more dynamic thing that makes it more challenging. (Consultant-2) [A director should be someone] who understands technology, who has done and overseen cybersecurity, so a former CIO, or a former CSO, somebody who has sat in the chair and has asked

	those questions of a CSO, or been in the operations seat and has done these things before. Otherwise, you run the risk of getting snowed, and you're going to." (Consultant-7) [In response to how oversight is different if there is a board with expertise] Well, I mean, to be crude, to not get bullshitted in a meeting, right? So if, if either one of you two are sitting in a meeting, a cyber meeting, and you see a board-level presentation, which is generally going to be fairly high level. But you're going to know the right kind of questions to start asking. You hear something in that presentation where it feels like, "Well, that feels a little weak," or "I'm not seeing something that I would expect to see in a cyber protection program here." …You bring somebody in, who's got real cyber expertise. I think that is a big risk mitigated for the board. (Executive-8)
4.2.3 Expertise enables board members to challenge the CISO	
	[Without a director with expertise,] I would predict that there wouldn't have been somebody in the audit and finance committee who would've stepped up, because they're already busy. They got a lot to do. I would bet that somebody else, one of the other board members, would've asked the question …, "So what are you guys doing about cybersecurity?" We would've had to go in and present, but it would've been at a much higher level. [Without the director with expertise] I don't know that we ever would've had this maturity model in place. … [C]ertainly we wouldn't have done that third party review and bring that in.… I think we would be at a very different [level]... I think it took an IT person to be able to really drill in and understand at the level she wanted to. I don't think the others would just have the interest. They would just want to know it's protected, and, "Do you have somebody in charge of it," or, "Do they know what they're doing," kind of thing. (Executive-2) In asking the CISO these questions, it was pretty clear the CISO was very old fashioned and was much more focused on keeping things out as opposed to assuming that people got in… And we ended up replacing that person. (Director-11) I think having people now on the boards that have that expertise is a risk mitigator for companies because it really is allowing subject matter expertise on the board to go. "We'll pull out here." [As an example of director feedback] "No, you're not making the right investment," or "You're not making the right level of investment." Or, "It's clear to me that the IT leadership in this company doesn't have the expertise needed to deal with the risks that are facing this company." And I think that's the value of having a board member that understands the cyber space. (Executive-8)
4.2.4 Expertise influences directors' proactive engagement	
	[Our more expert director] understands the ins and outs, and she's taken a liking to it. So she brings to the table a lot of things that we don't think about, and then she says, "Well, have you thought about this? Have you thought about that?" And that has been a godsend. (Director-1) [An experienced director] said, "I'd like to see a third party brought in, somebody from the outside, to do an independent assessment of where you are from a cyber maturity perspective and then put together an initiative plan so we understand where you're going and what things you're doing." So we said, "All right." We wanted to proactively get in front of that. (Executive-2) [T]he audit committee chair said, "I would like to do a benchmark and analysis using the same yardstick, the same measuring stick, to see how one [company] stacks up against the other, where we're strong, where we're weak, where there's synergies, where there's big gaps." And that launched our whole project. …Oftentimes, that is where it comes, is at the request of one board member who is seen as the IT or cybersecurity expert who can ask for those special things that sends the CISO or the CIO, or the chief risk officer, or the chief legal officer off to do these reports or these sorts of analyses. (Consultant-7)

Table 6 Additional Interview Evidence of Whether Cybersecurity Expertise is Needed

Is cybersecurity expertise needed?	
Yes	Having your own board member who is [themselves] an expert, in terms of the issues being discussed or presented, when the presenting CISO goes out of the room or looks away, [board members] can all look to you and say, "thumbs up?," ... [I]t's an extra little piece of validation, separate and independent of what their own personal entities might bring to the table. (Executive-7) [T]he board's chock full of all sorts of people who have run large businesses and understand governance and understand strategy and financial management systems and supply chains and all those things. And they're brought in because they had that experience. Why would you not do the same thing in your digitized space? Why wouldn't you bring somebody in that has that kind of expertise and knowledge, because in most corporations, that is the area where they are potentially the most singularly at risk for catastrophic failure. (Executive-8) I actually am very much an advocate of having a strong cyber presence on the board.… [T]here's virtually no industry that's untouched by [cybersecurity] anymore, and it's not going to get better in the short term. So I do support that approach and that regulation moving forward because I think the vast majority of boards are woefully—and this is from talking to peers and others—are inadequate in the space. I do support it. (Executive-9)
Middle ground	There's a lot of debate out there about boards having a designated cyber expert. I'm in the camp of, it depends. It depends on what kind of company it is. But definitely, the board has to have enough knowledge to understand risk presented by cyber risk, and then have confidence that management is executing to mitigate that risk. (Executive-6) I think when you look at the board and the function of the board, you really want people that are very broad based in knowledge. And not necessarily deep expertise. The most important role of the board is that financial fiduciary responsibility. Certainly, you're going to have accounting and audit practitioners and things like that.... [W]hen you give a board seat that's dedicated to technology, or cyber, or some combination [thereof]..., is that really benefiting the entire company? And for a technology company, it's probably yes. Certainly in fact, most board members of a technology company ought to be somewhere out of the technology sphere. But we're not a technology company, although we're obviously more and more dependent on technology. (Executive-6) I'm not opposed to [having a cybersecurity expert on the board], but I think that the board having the ability to directly contract for ancillary support is probably a shorter-term solution. I think in a long-term solution, I think that's a great idea. But again, I wouldn't just put a cybersecurity person in there. I would put somebody in there who understands the holistic environment of security and risk. (Consultant-5)
No	The shareholders do not expect their board members to be experts in cybersecurity. They expect the company to have experts in cybersecurity and to be effectively deploying those to manage the risks, and I think the boards rely on third parties much like we do in an audit. (Director-4) I think that for the level of oversight that they're providing, that just to have a general understanding of awareness is important. I'm not necessarily sure if they have to have a deep level. (Executive-3)

Table 7 Additional Interview Evidence of What Qualifies as Expertise

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

Appendix A. Sample of Questions from Semi-Structured Interviews

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

What does "cybersecurity risk" mean to you?

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

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

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

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

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

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

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

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

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

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

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