Firm Transparency of Risk Oversight:

An Examination of Cybersecurity Governance Disclosures

A Dissertation Presented for the

Doctor of Philosophy

Degree

The University of Tennessee, Knoxville

Laurie E Ereddia

May 2023

Acknowledgements

I am grateful for the support and encouragement from my dissertation committee: Lauren Cunningham (chair), James Myers, Justin Short, and Celeste Carruthers. I especially thank Lauren for her mentorship throughout my time in the program. Lauren inspires me daily and I am thankful to have such an incredible role model, coach, and friend. I also thank Linda and James Myers for their guidance, friendship, and hospitality. I am forever appreciative that they invited me to join this amazing Tennessee family. I am also grateful for the support and encouragement from my fellow doctoral students (Xi Ai, Nico Arguello, Jason Ashby, Jack Badger, Jason Bangert, Andrew Doucet, Audree Duncan, Travis Foshag, Kory Maag, Fellipe Raymundo, Stefan Slavov, Eric Stakebake, and Danielle Stanley).

I thank workshop participants at the University of Tennessee, Mississippi State University, Washington and Lee University, and Clemson University for helpful comments and suggestions on this dissertation. I am also grateful for the generous financial support from the University of Tennessee, the Haslam College of Business, and the Department of Accounting and Information Management, the Accounting Doctoral Scholars Program, and the AICPA Foundation. Finally, I thank my family for their unwavering support over the last four years. Most especially, I thank my mom, Miriam Hobbs, for her guidance and encouragement during this incredible journey.

Abstract

In this study, I examine factors associated with firm transparency of board oversight using the setting of cybersecurity risk. The SEC requires that, to the extent cybersecurity risks are material, firms must disclose the nature of the board's role in overseeing the management of that risk, allowing investors to assess how the board is fulfilling its risk oversight duties. Using textual analysis, I identify 2,921 firms that report material cybersecurity risk factors in their annual reports. From these firms' 2021 proxy statement filings, I hand collect data relating to 12 different elements of cybersecurity board oversight and create an overall Transparency Score (*T-Score*). Surprisingly, I find that over 36 percent of firms provide no information about the board's role in overseeing cybersecurity risk, even though these firms disclose material cyber risks in SEC filings. In multivariate analysis, I find that the level of disclosure relating to board oversight is positively associated with levels of cybersecurity risk, firm size, holdings by institutional investors, and board resources. I further find higher levels of disclosure when the full board shares oversight responsibility with a committee, or when a separate risk committee is tasked with oversight responsibility. Finally, I find that these determinants are generally stronger for firms that lack separate risk committees, as well as for those firms that have not previously reported a breach. These findings provide rich, descriptive evidence regarding transparency of risk oversight in an area that is timely and salient to investors, regulators, and other market participants.

Table of Contents

List of Tables

List of Figures

Section 1. Introduction

Market participants desire timely, high-quality, and useful information to assess risks and to make investment decisions (Munter 2021). Among the top concerns facing firms today, cybersecurity threats have grown more costly and pervasive.[1] According to a 2021 survey of executives, 72 percent of respondents indicate that their firms have recently experienced between 1 and 10 cyber incidents and data breaches in the previous year (Deloitte 2021). In addition to experiencing disruptions to operations, firms incur costs associated with the loss of intellectual property, lawsuits, regulatory fines, as well as reputational damage, with estimated losses to U.S. firms exceeding $6.9 billion in 2020 (FBI 2021; Perols and Murthy 2021; SEC 2022). As firms face increasingly complex threats relating to data security, boards must exercise significant oversight effort to ensure that networks, devices, and data are protected from unauthorized access (NACD et al. 2021). Board members invest considerable time and resources to improve the safeguards around firms' networks and data (EY 2021; PwC 2022). Because cybersecurity is quickly becoming one of the top risks facing firms, and because boards have an obligation to oversee significant risks, I use this setting to identify determinants of firm transparency around board oversight. Specifically, I examine firm characteristics that are associated with the extent to which firms choose to disclose matters relating to governance over cybersecurity risk.

The year 2020 was record-setting when it comes to data lost in breaches, as well as the number of cyber-attacks on firms, government agencies, and individuals (Brooks 2021). Risks continued to escalate during 2021 due to the COVID-19 pandemic, the rapid shift to a remote

[1] The U.S. Securities and Exchange Commission (SEC) describes cybersecurity as "…the activity or process, ability or capability, or state whereby information and communication systems and the information contained therein are protected from and/or defended against damage, unauthorized use, modification, or exploitation" (SEC 2018). Cybersecurity threats include data breaches, email phishing, spoofing, social engineering, ransomware, spyware, denial of service attacks, etc.

workforce, the increased use of cloud-based centers, more sophisticated hackers, and an increase in foreign actors attempting to disrupt world economies (SEC 2022a). In 2021, the FBI reported 7 percent more incidents than in 2020, with the most common related to ransomware, business email compromise schemes, and criminal use of cryptocurrency (FBI 2021). News headlines reporting far-reaching data breaches draw attention from the media, investors, and policymakers, putting pressure on firms to reexamine their cybersecurity risk management practices (Wickline 2021).[2] Furthermore, Amir et al. (2018) and Richardson et al. (2019) find negative stock price reactions to the disclosure of breach incidents, suggesting that these events harm shareholder value. Although it is management's responsibility to identify, assess, and manage risks, the board of directors has a duty to oversee risk management by evaluating the company's risk profile, determining whether the firm's strategy is aligned with the risk profile, and ensuring that ongoing risk management processes (e.g., company culture, managerial skills, internal controls, communication channels, etc.) are appropriate and effective (Larcker and Tayan 2020). My study examines the transparency of the board-level oversight of cybersecurity risk.

Broadly, the SEC requires that all firms provide information related to the board's oversight of the risk management process in its proxy statement. This disclosure should include "how a company perceives the role of its board and the relationship between the board and senior management in managing the material risks facing the company" (SEC 2009). The SEC first issued rules specifically targeting cybersecurity disclosure in 2011, and later provided additional interpretation in 2018. At a minimum, firms reporting material cybersecurity risk are required to

[2] Examples of recent data breaches attracting great attention include those at Equifax, SolarWinds, and Colonial Pipeline. See https://www.npr.org/2019/07/22/744050565/equifax-to-pay-up-to-700-million-in-data-breach-settlement, https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack and https://www.wsj.com/articles/colonial-pipeline-ceo-tells-why-he-paid-hackers-a-4-4-million-ransom-11621435636.

discuss the board's role in overseeing the management of cybersecurity, including information about the firm's cybersecurity risk management program and how the board engages with management on these issues (SEC 2011; SEC 2018). Policymakers have recently introduced new cybersecurity disclosure requirements, with the goal of increasing transparency over risk oversight practices, in particular (Nicodemus 2022). In a 2022 speech discussing proposed cybersecurity disclosure rules, SEC Chairman Gary Gensler stated that "companies and investors alike would benefit if this information were required in a consistent, comparable, and decision-useful manner" (Gensler 2022). Because information relating to cybersecurity risk oversight (CRO) is critically important to investors, regulators, and other stakeholders, my study examines the factors prompting firms to provide disclosure about CRO just prior to these proposed rule changes.

To investigate transparency of CRO, I examine firms' DEF 14A (proxy) filings because the SEC requires that firms provide information relating to the board of directors' role in risk oversight in this filing (SEC 2009). I select proxy statements filed in 2021 because this period follows a record-setting year in reported data breaches, while preceding potential SEC disclosure rule changes relating to cybersecurity risk. To ensure that the boards of my sample firms have a clear duty to specifically oversee *cyber*-related risk, I use Python script to identify firms with material cybersecurity risks reported in the Item 1A Risk Factor sections of the 10-K annual reports immediately preceding the proxy filings. For the 2,921, or 92 percent, of firms reporting a cybersecurity risk in Item 1A, I then hand collect data from the related proxy filings. Specifically, I collect data relating to 12 elements of board oversight, including how CRO is allocated across the board, director cybersecurity qualifications, how management engages with the board, as well as other details related to the firm's cybersecurity risk management program

(e.g., third-party audit or assessment of program, use of an external framework, cybersecurity insurance coverage). I find that over one-third of firms reporting material cyber-risks are silent on all matters relating to CRO, suggesting that it is this dearth of information that has attracted the SEC's recent attention. I further find that firms provide investors information relating to only 1.6 of 12 CRO program elements, on average.

Descriptively, I find that 42 percent of firms in the full sample fail to disclose how CRO is allocated across the board, which is a minimum expectation based on SEC risk oversight rules (SEC 2009). Among those that do disclose allocation of CRO, slightly more than 10 percent recognize CRO as a full board responsibility, 27 percent of boards delegate CRO to a committee, and 20 percent share the responsibility between the full board and a committee. Pertaining to committee assignments, a clear majority of firms assign CRO to the audit committee (77 percent), whereas others assign it to a risk committee (16 percent), to a technology committee (5 percent), or other committee (4 percent).[3] Relating to director qualifications to oversee cyber risk, I find that only 41 percent disclose some type of expertise or specialized training, suggesting that more than half of firms fail to provide shareholders with comfort that the board has adequate expertise to oversee management on this risk.

Relating to how senior management engages with the board in managing material cyber-risks, required by SEC disclosure rules, I find that only 20 percent of firms share communication channel information (e.g., the frequency of reports or meetings, the parties involved, etc.) that provides updates to the board on matters relating to cyber incidents, risk assessments, and various control activities. Finally, relating to the oversight processes, I find low levels of overall transparency. For example, 7 percent disclose that they conduct penetration tests to assess

[3] Note that 2 percent of firms assign CRO to more than one committee; therefore, these percentages add up to greater than 100 percent.

business readiness, should an incident occur, 9 percent discuss workforce training programs to increase awareness of cybersecurity threats (e.g., phishing, spoofing, etc.), 5 percent disclose the application of an external framework (e.g., NIST, ISO 27001, etc.), and 2 percent report that they align executive incentives with data security performance. Surprisingly, only 7.4 percent of firms disclose hiring external parties to review or provide assurance over their cybersecurity risk programs. Finally, I find that only 5 percent disclose that they carry cybersecurity insurance to mitigate the costs associated with potential breach incidents, suggesting that firms may not disclose such coverage to reduce exposure to litigation risk. Overall, firms' silence on the board's oversight processes makes it difficult for shareholders to hold directors accountable and likely motivates the SEC's proposed enhanced cybersecurity disclosure rules to close this disclosure gap.

Next, I use the hand-collected data to examine the determinants of firm transparency around risk oversight. Beginning with the level of cybersecurity risk, I identify high-risk industries using the proportion of firms that report a data security breach in the three-year period preceding my sample period. Although firms operating in high-risk industries may desire to increase investor confidence by providing greater information relating to their cyber-risk preparedness, firms may also perceive greater risk by providing too-detailed information, potentially increasing cyber-risk exposure. Therefore, I do not make a prediction relating to the association between levels of cybersecurity risk and CRO disclosure. Next, I consider factors relating to stakeholder demand for risk oversight disclosure using firm size and the level of holdings by institutional investors. Finally, I consider board resources, examining the influence of board size, boards with directors serving concurrently on multiple boards, the presence of directors with technology expertise, and auditor size on CRO disclosure. I predict that factors

relating to stakeholder demand and board resources will be positively associated with CRO disclosure.

In the main model, I examine the determinants of transparency relating to four different disclosure decisions: CRO allocation across the board, director CRO qualifications, CRO reporting from management to the board, and at least one other process or activity used to oversee cyber risk. After controlling for fundamental firm characteristics, I find that firms operating in high cybersecurity risk industries are more likely to disclose three of the four CRO elements. Surprisingly, I find no association between firms operating in high cyber-risk industries and the disclosure of related director qualifications. I further find, across each of the four disclosure decisions, positive associations with stakeholder demand, suggesting that it may take external pressure to prompt firms to provide the desired information. Relating to board resources, I find consistent support that larger boards, those with directors sitting on multiple boards, and boards with IT-expert directors are all more likely to provide these four CRO disclosures. Finally, I find some evidence that engaging Big 4 auditors is associated with CRO disclosure overall. Specifically, I find that the disclosure of the two items that most closely correspond with current SEC requirements, CRO assignment and CRO reporting from management to the board, both are positively associated with Big 4 auditors, whereas disclosure relating to director qualifications and CRO processes are not.

Next, I aggregate the 12 cybersecurity oversight elements to create an overall Transparency Score (*T-Score*) and examine firm characteristics that promote *the extent to which* firms provide stakeholders information in this critical area of board oversight. In the full sample, I find that the level of overall disclosure continues to be positively associated with cybersecurity risk, demand for disclosure, and board resources; however, I find no association between *T-Score*

and use of Big 4 auditors. Next, I consider whether *the nature of* CRO allocation across the board influences CRO disclosure decisions. I find that firms with full boards *sharing* CRO responsibility with a committee are more transparent, as compared to firms whose boards fully retain responsibility, as well as those boards that fully delegate CRO to specified committees. Finally, I examine whether the type of committee assignment influences CRO disclosure decisions, relative to firms with boards that retain CRO responsibility. I use a reduced sample of only those firms that disclose CRO assignment and include indicator variables for each committee assigned CRO. I find that boards that delegate CRO to the risk committee provide more transparency, as compared to those that delegate CRO to the audit committee, the technology committee, or another named committee. These results are robust to alternate versions of *T-Score*, as well as principal component analysis. Finally, in cross-sectional analyses, I find that these determinants have a greater impact, on average, for firms that have formed separate risk committees, as well as for firms that have not previously reported a data security breach.

My study contributes to the literature in several ways. Broadly, my paper contributes to the literature on cybersecurity risk and disclosure by providing rich and descriptive information related to governance disclosure in an area of significant stakeholder interest. Although prior studies have focused on cybersecurity risk factor disclosures in annual reports (Gordon et al. 2006; Brown et al. 2018; Jiang et al. 2022), I expand this literature stream by examining the information firms provide stakeholders regarding how the board fulfills its oversight duties in this critical area of risk. Next, by examining factors that influence disclosure decisions, I contribute to the broader disclosure literature (Healy and Palepu 2001; Hermalin and Weisbach 2012; Leuz and Wysocki 2016). These findings are relevant to practitioners interested in current

cybersecurity governance disclosure practices, as well as to policymakers considering new cybersecurity-related disclosure rules. Furthermore, I recommend that future research in this emerging literature stream take into consideration the determinants identified in this study as potential confounding effects of board oversight disclosure decisions. Finally, given the ongoing debate surrounding the SEC's proposed cybersecurity disclosure rule changes, this study provides insights relating to factors influencing firm disclosure prior to these proposed rules, allowing future research to examine whether, and to what extent, the new rules have an impact on firm disclosure decisions.

The remainder of the paper is organized as follows. Section 2 discusses the background and prior literature related to cybersecurity risk, board oversight, and related disclosure. In Section 3, I discuss the research design and develop predictions for the determinants in my models. I describe the data and sample characteristics in Section 4. In Section 5, I present the main results and additional analyses. Section 6 concludes the study and discusses opportunities for future research.

Section 2. Background And Prior Literature

2.1. Cybersecurity Risk

In a 2012 speech, former FBI director Robert S. Mueller declared that "there are only two types of companies: those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again" (Mueller 2012). Cybercrime continues to increase over time, quickly becoming a top concern facing management and boards. The FBI Internet Crime Complaint Center (IC3) reported a 300 percent increase in the number of cybersecurity complaints submitted from 2019 to 2020, as the pandemic forced many activities to shift online, exposing new vulnerabilities and leading hackers to seek ways to exploit those vulnerabilities (Miller 2020). The year 2020 was record-breaking in data breach incident activity (Brooks 2021). Several factors have contributed to this rapid rise in cyberattacks. Threats have intensified due to the amount of data migrating to the cloud, firms introducing new customer-facing technology, a greater proportion of the general workforce accessing data remotely and on personal devices, while hackers have become more sophisticated over time (Deloitte 2021).

The cost associated with data breaches is significant. For example, in 2017, Equifax experienced a massive data breach, where hackers compromised personal information, including social security numbers, birthdates, addresses, and in some cases driver's license numbers, belonging to nearly 150 million people (Schneider and Arnold 2019). The Federal Trade Commission (FTC) alleges that Equifax failed to patch a critical network vulnerability, allowing multiple hackers to access sensitive information over several months (FTC 2019). In addition to experiencing reputational damage, Equifax agreed to pay over $575 million in fines and in

monetary relief to affected consumers, and to implement comprehensive changes to its cybersecurity program (FTC 2019).

The stakes continue to grow for firms and investors, as well as for governmental and not-for-profit entities. In 2020, Texas firm SolarWinds experienced a sophisticated breach that allowed hackers access to its 18,000 clients, including many Fortune 500 firms, governmental agencies, hospitals, and universities (Canales and Jibilian 2021). In this "worse nightmare" breach, hackers were able to add code to SolarWinds' Orion software, creating a backdoor to its customers' IT systems, and allowing the hackers to install malware to spy on firms (Temple-Raston 2021). Among those affected were Microsoft, Intel, Deloitte, the U.S. Treasury, and the Pentagon (Poulsen et al. 2020). In 2021, Colonial Pipeline suffered a ransomware attack that shut down a pipeline that transports over 45 percent of the fuel to East Coast states (Eaton and Volz 2021). Recognizing that the hack was causing damage to the U.S.'s "critical energy infrastructure," Colonial Pipeline issued a ransom payment of $4.4 million in bitcoin to restore the pipeline services (Eaton and Volz 2021).

With this increase in reported incidents has also come a rise in media attention on data breaches. Using RavenPack News Analytics data, Figure 1 presents the number of firm-specific news articles relating to cybersecurity breaches, increasing from 7 in 2004 to nearly 2,500 in 2021.[4] Prior studies find that investor and media attention is associated with executive leadership and corporate governance changes (Farrell and Whidbee 2002; Iliev et al. 2021; Guernsey et al. 2022), suggesting that there are penalties for ineffective oversight and the unwanted media attention that follows. Because data breaches can have far-reaching impact for businesses,

[4] According to the RavenPack User Guide: "RavenPack News Analytics – Dow Jones Edition analyzes relevant information from Dow Jones Newswires, regional editions of the Wall Street Journal, Barron's and MarketWatch. With more than 5,000 employees around the world, including more than 2,000 journalists in 58 countries, Dow Jones publishes the world's best business and financial news" (RavenPack News Analytics 2016).

investors, consumers, suppliers, not for profits, as well as government agencies, incidents will continue to receive significant media attention, putting pressure on firms and boards to improve oversight and to provide stakeholders information related to their strategy to oversee these risks.

2.2. Cybersecurity Disclosure

Regulation S-K broadly requires that firms disclose in annual reports any material risks to operations that make an investment in the registrant speculative or risky, as well as the extent of its board of directors' role in risk oversight (SEC 1975).[5] In 2011, in response to increased attention on cyber attacks, the SEC released the first disclosure requirements explicitly related to cybersecurity.[6] According to these rules, both domestic and non-U.S. issuers should include cybersecurity risks in Item 1A Risk Factors in annual filings if these risks are significant factors that could substantially impact investors, and firms should describe their analyses of these risks, including the probability and potential magnitude of those risks, using specific, non-general language (SEC 2011). While the 2011 SEC rules explicitly require disclosure of material cybersecurity risks and incidents in financial statements, they do not address disclosure requirements relating to the governance over cybersecurity risks.

In 2018, the SEC issued a new statement that provided interpretive guidance relating to disclosure of cybersecurity controls and procedures (SEC 2018).[7] Expanding on both the 2009 proxy disclosure enhancement rules, as well as the 2011 cybersecurity disclosure rules, this statement stresses disclosure obligations across all regulatory filings. Relating to proxy filings, it requires that, to the extent that cybersecurity risks are material to a firm's business, firms provide

[5] Also see Item 407(h) of Regulation S-K: https://www.law.cornell.edu/cfr/text/17/229.407.
[6] For additional information related to the SEC's 2011 cybersecurity disclosure guidance: Topic No. 2, see: https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.
[7] For additional information related to the SEC's 2018 statement and guidance on public company cybersecurity disclosure, see: https://www.sec.gov/rules/interp/2018/33-10459.pdf.

information about the nature of the board's role with regard to cyber-risk oversight, as well as how the board of directors engages with management on cyber-related matters (SEC 2018). The SEC further stressed that this information was important for investors to assess how the board is fulfilling its cyber-risk oversight duties. However, beyond allocation of CRO and related the reporting between management and the board, the SEC's 2018 cybersecurity guidance does not explicitly name which program elements must be disclosed, allowing firms flexibility relating to the nature and the extent of the information provided to stakeholders.

In early 2022, in an effort to provide investors with more "consistent, comparable, and decision-useful disclosures," the SEC proposed new requirements related to firms' cybersecurity risk management policies and practices (SEC 2022).[8] Specifically, the proposal requires that firms file a Form 8-K within four business days of a "material" cybersecurity incident, to provide updates related to previously reported material breaches, and to disclose specific elements related to the board's oversight of cybersecurity risk (SEC 2022). Related to board oversight, the proposed rules explicitly require disclosing whether the full board or a specified committee are responsible for overseeing cybersecurity risks, the process and frequency of reporting to the board related to cybersecurity risks, as well as how the board considers cybersecurity risks in its overall risk oversight strategy. Finally, the proposed rules require that firms disclose the level of board member cybersecurity expertise, including the name of each director with cybersecurity expertise, as well as a description of the director's expertise. The SEC first released the proposed rules on March 9, 2022, allowing a two-month comment period, and was among the rulemaking releases that saw its comment period reopened in October due reported "technological errors" at

[8] For additional information related to the SEC's 2022 *proposed* cybersecurity risk management, strategy, governance, and incident disclosure, see: https://www.sec.gov/rules/proposed/2022/33-11038.pdf. As of February 1, 2023, these rules have not yet been adopted.

the SEC (SEC 2022c). As of February 1, 2023, the SEC has received 196 comment letters related to the proposed rules. Initial comments from preparers, auditors, and academics provide cautious support for the new rules. [9]

2.3. Prior Literature

Stakeholder demand for disclosure arises from information asymmetry inherent in agency conflicts between insiders and outsiders (Fama 1980). Specifically related to cybersecurity risk and disclosure, prior literature examines disclosure decisions relating to data security risks in Item 1A Risk Factors of a firm's annual report (Gordon et al. 2006, 2010; Brown et al. 2018), factors relating to the likelihood of a data breach (Steinbart et al. 2012; Wang et al. 2013; Higgs et al. 2016; Lending et al. 2018; Li et al. 2018; Vincent et al. 2019) and outcomes following data breach incidents (Kashmiri et al. 2017; Martin et al. 2017; Amir et al. 2018; Jeong et al. 2019; Richardson et al. 2019; Lankton et al. 2021). In a recent review of the literature, Walton et al. (2021) find two streams related to cybersecurity disclosure – studies that examine the determinants of disclosed risk factors and studies examining the impact of cybersecurity risk disclosure. Related to the determinants of disclosed risk factors, prior studies find that regulator attention is positively associated with information security disclosure (Gordon et al. 2006; Brown et al. 2018).

Two most closely-related studies examine firm disclosures relating to board oversight of cybersecurity risk using a small sample of Canadian firms. Héroux and Fortin (2020) examine firm filings (i.e., annual information forms, annual and quarterly management's discussion and analysis, proxy statements, material change reports, and press releases) for firms comprising the S&P/TSX 60, a Canadian index of the Toronto Stock Exchange (TSX), from January 2017

[9] To view comments related to the SEC's 2022 proposed cybersecurity risk management, strategy, governance, and incident disclosure, see: https://www.sec.gov/comments/s7-09-22/s70922.htm.

through mid-2018 to determine the extent to which firms comply with Canadian Securities Administrator (CSA) guidelines. The authors collect data relating to disclosed risk factors, responsibilities, potential and actual breach incidents, and other items, finding considerable variation in the levels of detail provided by firms, as well as an overall low level of compliance level, and frequent use of boilerplate language. Smaili et al. (2022) examine annual reports for a sample of S&P/TSX 60 firms over the period from 2014 through 2018. They find a positive relation between a firm's decision to disclose cybersecurity information in the annual report and board independence and director financial expertise, whereas they find no relation between such disclosure and board size.

Because the firms in these two studies follow the standards as governed by the CSA, as well as those of the TSX exchange, it is unclear whether their findings are generalizable in the U.S. regulatory environment. Additionally, because my sample is comprised of nearly 3,000 firms, as opposed to the 60 firms in the Canadian studies, and because my sample has significant variation across firm size and industry, my study provides richer descriptive information that can also be examined cross-sectionally, making the findings more useful to practitioners, policymakers, and researchers.

Section 3. Research Design

As firms face heightened cybersecurity threats, and as current boardroom discussions increasingly consider ways to mitigate and to respond to these threats, investors and other stakeholders desire timely, high-quality, and useful information relating to board oversight in order to make informed decisions. Because little is known about firm disclosure choices relating to how the board is fulfilling its oversight duties, it is important to investigate factors that are associated with these disclosure decisions.

3.1. Determinants of Cybersecurity Risk Oversight Transparency

I investigate the factors associated with a firm providing board-level oversight information to stakeholders by examining proxy filings. I use proxy statements to collect risk oversight data because these filings are dedicated to governance-related disclosure, including the board's responsibility for risk oversight, director qualifications, executive compensation, and other information that aids shareholders' ability to make informed decisions when voting at the annual meeting.[10] Furthermore, the SEC explicitly states in its 2018 Cybersecurity Disclosure Guidance that, in accordance with Item 407(h) of Regulation S-K and Item 7 of Schedule 14A, firms should report matters relating to board risk oversight in the proxy filing (SEC 2018).

Model (1) estimates the probability of a firm disclosing CRO in its 2021 proxy filing, including the assignment of oversight responsibility, relevant director qualifications, reporting between senior management and the board on CRO matters, and any risk-mitigating processes or activities. To examine these determinants, I estimate the following model using a logistic regression:

[10] For general information relating to proxy statements (Form DEF 14A filings), see: https://www.investopedia.com/terms/p/proxystatement.asp

$$
\begin{aligned}
Disclose\_CRO_{\,i} = {} & \beta_0 + \beta_1\, High\_IndBreach_{\,i} + \beta_2\, FirmSize_{\,i} + \beta_3\, InstInvest_{\,i} \\
& + \beta_4\, BoardSize_{\,i} + \beta_5\, MultiBd\_Dir_{\,i} + \beta_6\, IT\_Expert_{\,i} + \beta_7\, Big4_{\,i} \\
& + \beta_8\, FirmAge_{\,i} + \beta_9\, ROA_{\,i} + \beta_{10}\, Growth_{\,i} + \beta_{11}\, Leverage_{\,i} \\
& + \beta_{12}\, Loss_{\,i} + \beta_{13}\, Returns_{\,i} + \beta_{14}\, MWeak_{\,i} + \beta_{15}\, Lit\_Indus_{\,i} \\
& + \beta_{16}\, Merger_{\,i} + \beta_{17}\, Foreign_{\,i} + \beta_{18}\, NYSE_{\,i} + \beta_{19}\, Length_{\,i} + \mathcal{E}_{\,i} \qquad (1)
\end{aligned}
$$

where *i* represents a firm and *t* represents a fiscal year.[11] In Model (1), the dependent variable *Disclose_CRO* represents one of four different disclosure outcomes. First, *Discl_Assign* is an indicator variable equal to one if a firm discloses how CRO is allocated to the board (e.g., to the full board, to a committee, shared between the full board and a named committee), and zero otherwise. Second, *Discl_Qual* is an indicator variable equal to one if a firm discloses that a current board member has work experience or certifications relating to technology or cybersecurity, and zero otherwise. Third, *Discl_Report* is an indicator variable equal to one if the firm provides information describing how senior management reports to the board on CRO matters, and zero otherwise. Finally, *Discl_Process* is an indicator variable equal to one if a firm discloses at least one CRO process element (e.g., use of a third-party advisor, alignment with an external framework, workforce training programs, cybersecurity insurance coverage), and zero otherwise.

I examine the determinants of CRO disclosure and consider factors relating to the level of industry-specific cybersecurity risk, to stakeholder demand for related oversight disclosure, and finally, to the level and types of board resources that firms have available to oversee cybersecurity risk.

[11] I do not add industry fixed effects because variance inflation factors (VIFs) exceed 10 when they are included in the model. Instead, I include *High_IndBreach* to capture firms operating in high-risk industries, identified using reported data breaches in the prior three years. In additional analysis, I rerun main tests including industry fixed effects and all inferences are unchanged.

3.2. Level of Cybersecurity Risk

When introducing the proposed cybersecurity disclosure rules, Chairman Gensler noted that the SEC's disclosure requirements evolve over time, in response to ever-changing risks and investor needs (Gensler 2022). It is in the context of increasing cyber-risk that the SEC finds an increasing investor need for information that gives them the ability to effectively assess how a board is overseeing cybersecurity risk (SEC 2022a). From a regulatory perspective, levels of risk and the quantity of information related to that risk needed by investors should be positively correlated. Firms that operate in industries more prone to cyberattacks and data breaches need to provide higher levels CRO disclosure to market participants. Prior literature also finds that firms providing more transparency are able to reduce information asymmetry and lower its cost of capital (Leuz and Wysocki 2016). Therefore, the amount of cybersecurity risk may be positively associated with CRO disclosure. However, prior research finds that a firm makes disclosure decisions based on private cost-benefit considerations (Hermalin and Weisbach 2012). Firms with higher levels cybersecurity risk may provide *less* information if the firm perceives that such disclosure might draw unwanted attention, aid hackers' ability to identify data security vulnerabilities, or increase its exposure to litigation risk.

To identify past data breaches, I use Audit Analytics' cybersecurity database, which reports breach incidents from 2010 through 2022. Because more recent breaches are likely to be most salient to firms, I limit the incidents to those reported from 2018 through 2021. I identify the industry-peer groups, using a 4-step process to ensure very precise peer groupings. I first use Hoberg-Phillips Text-based Network Industry Classifications (TNIC) data, which uses textual analysis of business descriptions from annual filings to construct pairwise similarity scores

between firms (Hoberg and Phillips 2010, 2016).[12] Slightly more than 70 percent of firms in my sample are matched with a sufficient number of peers using the TNIC similarity scores. For those firms that have fewer than 10 TNIC peers, I next use 4-digit SIC codes, followed by 3-digit SIC codes, and finally 2-digit SIC codes, requiring 10 or more peer firms before moving to the next lower-level of industry classification. Because firms with higher cybersecurity risk have competing incentives relating to levels of CRO disclosure, I do not make a directional prediction for *High_IndBreach*, an indicator variable equal to one if the proportion of industry-peer firms that have reported a data breach in the previous three years is greater than the median, and zero otherwise.

3.3. Stakeholder Demand for Oversight Information

Next, I consider the impact of stakeholder demand on disclosure decisions. Larger firms are more visible and face more pressure from proxy advisors, analysts, and the news media (i.e., a "spotlight effect") (Guernsey et al. 2022). Because a more visible firm incurs greater potential reputational and litigation cost should it fail to protect its network, software, and data, as compared to a smaller, less-visible firm, I predict a positive relation between CRO disclosure and *FirmSize*, measured using the natural log of the market value of equity. Next, I consider the influence of investors, which are key stakeholders that, in order to make informed investing decisions, pressure firms to provide CRO disclosure. Institutional investors, because of proportion of shares they hold and amount of market capital they control, can influence firm choices, including disclosure decisions (Bochkay et al. 2022). Therefore, I predict a positive relation between CRO disclosure and the level of institutional ownership, *InstInvest*, which is

[12] The Hoberg-Phillips TNIC data is calculated at a granularity level similar to that of 3-digit SIC codes. See https://hobergphillips.tuck.dartmouth.edu for further information.

equal to the percent of outstanding common shares owned by institutional investors at the end of the prior fiscal year.

3.4. Board Resources

Finally, I consider board resources and characteristics because these impact how a board fulfills its oversight responsibilities, as well as its governance disclosure decisions (Coles et al. 2008). Board resources can also represent capacity constraints on the levels of oversight activity and its related disclosure. Because larger boards represent higher levels of monitoring resources and knowledge, a larger board may choose to more fully disclose its oversight activities, as compared to a smaller board. Therefore, I predict a positive relation between CRO disclosure and board size, *BoardSize*, measured as the number of directors on a board. Next, I consider how directors serving concurrently on multiple boards might observe what information other firms provide in regulatory filings relating to risk oversight. These directors have the opportunity to identify disclosure best practices, especially in current "hot-button" topics such as cybersecurity, increasing the likelihood of disclosing information in this growing and critical area of risk oversight. Therefore, I predict a positive relation between CRO disclosure and boards with multiple-board-serving directors, *MultiBd_Dir*, calculated as the proportion of directors that serve on three or more concurrent boards at year end.

Next, I consider the role of cybersecurity specialists and financial reporting advisors. Because prior literature finds that boards with IT-expert directors have more mature IT risk management processes (Vincent et al. 2019), which would reasonably include disclosure practices, I predict a positive relation between CRO disclosure and IT expertise, *IT_Expert,* which is equal to one if at least one director on the board has past or current employment in a technology- or cybersecurity-related role, and zero otherwise. I identify directors with IT

expertise using BoardEx Individual Profile Employment data, and using keywords similar to Ashraf et al. (2020).[13] Relating to financial reporting advisors, I examine the type of independent auditor that the audit committee engages. Because external auditors act as an advisor to clients in disclosure decisions (Dunn and Mayhew 2004), and because audit firm size is associated with higher audit quality, of which disclosure quality is a component (DeFond and Zhang 2014), I predict a positive relation between CRO disclosure and use of a Big 4 auditor, *Big4,* which is an indicator equal to one if the firm retained a Big 4 auditor, and zero otherwise.

3.5. Control Variables

I recognize that these variables of interest are not exogenous choices for firms in my sample. Because there are fundamental firm characteristics that are likely correlated with both my variables of interest, and the firm's disclosure decisions, I include controls for firm characteristics relating to maturity, financial performance, risk, and complexity. Specifically, I control for maturity (*FirmAge*) using the natural log of the number of years the firm has existed within the Compustat database, profitability (*ROA*) using the ratio of net income before extraordinary items divided by average total assets, growth opportunities (*Growth*) using the market to book ratio, leverage (*Leverage*) using the sum of long-term debt and total current liabilities, scaled by total assets, negative net income (*Loss*), returns (*Returns*) using buy and hold 12-month returns, internal control material weaknesses (*MWeak*), an indicator equal to one if the internal control opinion is qualified opinion for a material weakness in the prior year, litigious industry (*Lit_Indus*), an indicator if the firm operates in a litigious industry, following

[13] Specifically, consistent with keywords in Ashraf et al. (2020), I search ROLENAME for "Chief Information Officer," as well as director-, vice president-, senior vice president-, head-, manager-, or general manager-level role in fields relating to information technology (i.e., "information technology," "information services," "information systems," "information management"). Because I am interested in director work experience that would aid a board in its cybersecurity oversight responsibilities, I also include ROLENAME keywords relating to data security, including "cybersecurity," (and variations thereof), as well as "data security," and "information security," director-, vice president-, senior vice president-, head-, manager-, or general manager-level roles.

Francis et al. (1994), mergers (*Merger*), an indicator equal to one if the firm engaged in a merger or acquisition in the prior year, and foreign income (*Foreign*), an indicator equal to one if the firm has pre-tax foreign income or loss in the prior year.

Because firms listed on the New York Stock Exchange (NYSE) must adhere to an additional set of governance rules, including the explicit requirement that the audit committee "discuss policies with respect to risk assessment and risk management" (NYSE 2014), I include an indicator variable (*NYSE*), equal to one for firms listed on the NYSE, and zero otherwise. To control for innate characteristics about the firm's disclosure strategies, I include the natural log of the word count of the most recent proxy statement, (*Length*).[14]

Because the dependent variables, measured in year *t*, relate to proxy statements, which are filed between the annual report filing date and the annual meeting date, explanatory variables are measured at the fiscal year end of the prior year, year *t*-1.[15] I winsorize all continuous variables at the 1 and 99 percent levels to reduce the influence of outliers. All p-values are based on two-tailed tests, except when there is a predicted sign, in which case I use one-tailed tests. Finally, all standard errors are robust to heteroskedasticity, following White (1980). All variables are defined in Appendix A.

3.6. Transparency Score (T-Score) Model

Next, I investigate the factors associated with *the extent to which* a firm provides information about oversight of cybersecurity risk. I estimate Model (1) using an ordinary least squares regression, and replace *Disclose_CRO* with a Transparency Score (*T-Score*), which is a

[14] It is possible that *Length* is a "mediator" control variable (Whited et al. 2022), biasing the coefficient estimates, because the length of a proxy statement necessarily increases as the level of CRO disclosure increases. However, CRO disclosures are brief, relative to the overall proxy statement, which houses other information related to executive compensation, auditor oversight, etc., limiting its influence in the measurement of *Length*.

[15] For example, Equifax filed its 2021 proxy statement on March 25, 2021, which served as the official notice of the 2021 annual shareholder meeting, scheduled on May 6, 2021. The independent variables are measured using Equifax's 2020 annual report for the year ending December 31, 2020, which was filed on February 25, 2021.

count variable ranging from 0 to 12, with 12 being the maximum number of risk oversight elements disclosed in a firm's proxy statement. Specifically, I identify cybersecurity program elements relating to:

1. The assignment of cybersecurity oversight
2. Director qualifications relating to cybersecurity
3. Reporting from management to the board on to cybersecurity matters
4. Specific cybersecurity program processes and activities
5. Workforce-level training activities
6. Involvement of the internal audit function
7. Alignment with an external framework
8. Use of a third-party to assess or audit the cybersecurity program
9. Collaboration with peer or industry groups
10. Use of cybersecurity insurance
11. Executive cybersecurity expertise
12. Executive compensation discussion includes statements relating to cybersecurity performance, achievements, or Key Performance Indicators (KPIs)

See Appendix B for further descriptions of the *T-Score* elements, as well as examples of each from 2021 poxy filings.

Using *T-Score* as the dependent variable, I examine the extent to which a firm provides information about CRO using a full sample. I next consider whether disclosure is influenced by the governance party assigned CRO responsibilities (i.e., retained by the full board, delegated to a specified committee, shared between the board and a committee), relative to firms that do not disclose CRO assignment. Finally, using a reduced sample of firms that disclose CRO assignment, I examine the whether the type of committee influences disclosure decisions, relative to firms where the full boards retain CRO responsibility.

Section 4. Data And Sample Characteristics

To investigate the determinants of a firm's transparency in matters relating to CRO, I examine proxy statements that were filed in 2021.[16] Because proxy statement data are not machine readable and require manual interpretation to properly classify the information, all analyses are based on hand-collected data. I select 2021 for the study sample because it follows the highest year on record for data breach activity and related media attention (Brooks 2021), and because it precedes the SEC (2022) rulemaking release relating to cybersecurity disclosure. Furthermore, in January 2021, Institutional Shareholder Services (ISS) released an update to its ESG Governance QualityScore methodology, adding cybersecurity governance factors, and putting further pressure on firms to improve transparency relating to board oversight of cybersecurity risk (McPhillips and Osea 2021).[17] Altogether, these events significantly increased the salience of oversight and transparency relating to cybersecurity risk for board members and stakeholders during the 2021 proxy season.

Using WRDS SEC Analytics Suite, I identify 5,386 annual meeting proxy statements filed between January 1, 2021 and December 31, 2021. Next, I merge the proxy statement data with data required for my analyses, including Audit Analytics, BoardEx, Compustat Fundamentals Annual, The Center for Research in Security Prices (CRSP), SEC Analytics Suite by WRDS, and Thomson Reuters Institutional (13f) Holdings. The resulting sample is comprised of 3,965 proxy statements filed in 2021. Because the SEC requires firms to provide information in its proxy statement relating to board oversight of "material risks facing the company" (SEC

[16] Because the nature and purpose of special meetings can vary considerably, I include in my sample only proxy statements related to annual meetings and exclude any filings related to special meetings.

[17] ISS describes its ESG Governance QualityScore as "a data-driven scoring and screening solution designed to help institutional investors monitor portfolio company governance. At both an overall company level and along topical classifications covering board structure, compensation, shareholder rights, and audit & risk oversight, scores indicate relative governance quality supported by factor-level data." For further information on ISS's QualityScore, see: https://www.issgovernance.com/esg/ratings/governance-qualityscore/.

2009), I limit my sample to those firms that have disclosed a cyber-related risk in its Item 1A – Risk Factors in its annual report immediately preceding the 2021 proxy statement. If a firm discusses a cybersecurity-related risk as material in its annual report, it suggests that a board of directors has a duty to carry out related oversight responsibilities, allowing me to measure the extent to which the firm provides stakeholders information relating to the nature of those oversight activities.

Using a method similar to that found in prior research (Dhaliwal et al. 2013; Gaulin 2017; Li et al. 2018), I use Python script to extract text from the Item 1A – Risk Factor footnote in annual reports, and search for keywords relating to cybersecurity, data privacy, and data breaches.[18] I find that 92 percent of firms include at least one cybersecurity-related risk.[19] Finally, I remove observations missing data necessary to estimate my main model (1). The resulting sample is comprised of 2,921 firms with a material cybersecurity risk and a 2021 proxy statement. From these filings, I manually collect data relating to the board of directors' allocation of CRO across the board and its committees, director cyber-related qualifications, how management reports to the board on CRO matters, as well as the processes and procedures that have been implemented in response to cybersecurity risk. In all, I collect 12 elements of CRO to construct *T-Score*.[20] Table 1, Panel A presents my sample construction process.

[18] Specifically, I extract text from 10-K filings beginning with Item 1A and ending with Item 1B or Item 2 using Python and the Beautiful Soup parsing package. Next, I broadly search within the Risk Factor text for keywords including "cyber," "data security," "information security," "data breach," "security breach," and "privacy breach."
[19] This proportion is in line with Li et al. (2018), which uses a similar textual analysis methodology to examine firms disclosing cybersecurity risk factors in 10-Ks and find an increasing proportion of firms disclosing these risks from 2007 through 2015, with 72.7 percent including cybersecurity risk factors in Item 1A in 2015, the final year of its sample. As expected, the percentage increased from 2015 to 2020.
[20] To identify the 12 categories of CRO, I read an initial 100 filings, collecting approximately 30 items from each filing to become familiar with common practices in the 2021 proxy season. Next, I identified the broader categories that would be most salient to stakeholders, including the specific categories named in the SEC proposed rules, and selected 12 elements to continue collecting going forward. I then employed three graduate student research assistants to continue the remaining data-collection process, reviewed their data collection, and provided guidance, as needed.

Table 1, Panel B presents the distribution of the full sample of observations across industries, defined using the Fama-French 12 industry classification. The three industries with the highest number of observations in the sample include Financial Institutions (26%), Healthcare, Medical Equipment, and Drugs (19%), and Business Equipment (15%). Firms, on average, disclose 1.6 elements of risk oversight (*T-Score*) in their 2021 proxy statements. On average, firms operating in the Utilities industry disclose the most elements (2.54), whereas firms operating in the Healthcare, Medical Equipment, and Drugs industry disclose the least number of elements (0.90). It is surprising that healthcare firms, which store vast amounts of highly sensitive and personal data, share the least amount of information relating to board oversight and the safeguards over consumer data.

Table 2, Panel A presents descriptive statistics. I find that 58 percent of firms disclose how they allocate CRO across the board (*Discl_Assign*), 41 percent disclose relevant board member cybersecurity qualifications (*Discl_Qual*), 20 percent disclose how management reports to the board on CRO matters (*Discl_Report*), and 22 percent disclose at least one other element relating to its cybersecurity program (*Discl_Process*). By variable construction, half the firms in my sample operate in high-risk industries, based on previously reported breaches (*High_IndBreach*). The average firm in my sample is relatively large, with a market capitalization of $1.39 billion (the natural log of 7.24 million) (*FirmSize*), and with 60 percent of shares held by institutional investors (*InstInvest*). Relating to board characteristics, the average board has slightly fewer than 9 directors (*BoardSize*), with an average of 44 percent of their members serving concurrently on at least three boards (*MultiBd_Dir*), and 21 percent of the directors having cyber- or IT-relevant work experience (*IT_Expert*). Finally, 69 percent of firms in the sample engage Big 4 auditors for financial statement audits (*Big4*). Relating to firm

fundamental characteristics, the average firm in my sample is relatively mature, at approximately 17 years old (the natural log of 2.85) (*FirmAge*), and has mixed financial performance (*ROA, Growth, Leverage, Loss, Returns*). Relating to risk, only 4 percent of firms previously reported material weakness in internal control (*MWeak*), whereas almost one-third of firms operate within litigious industries (*Lit_Indus*). Relating to complexity, one-third of firms in my sample have completed a merger or acquisition in the prior year (*Merger*), and half report foreign income (*Foreign*). Finally, 41 percent of firms are listed on the NYSE (*NYSE*). Untabulated, 12.6 percent of firms have separate risk committees, and 8 percent firms have reported a data breach in the previous three years.

Figures B – C provide additional descriptive information relating to the variation of how firms allocate CRO across board parties. Using the full sample, Figure 2 presents the proportion of firms that the responsibility of CRO is retained by the full board (10 percent), delegated to a specified committee or committees (27 percent), and shared by the full board and a specified committee (20 percent). However, out of 2,921 observations, 42.4 percent of firms are silent in this matter. Figure 3 presents, of firms that indicate that a committee assignment relating to CRO responsibility (N = 1,378), to which committee CRO is assigned. I find that 77 percent of firms assign CRO to the audit committee, 16 percent assign CRO to the risk committee, and 5 percent assign CRO to the technology committee. Approximately 4 percent of firms have a specialized committee (e.g., cybersecurity-specific committee) that are assigned CRO responsibility.[21]

Next, Figure 4 presents the frequency of firms that disclose each of the 12 elements that comprise *T-Score*. Using the full sample of firms, I find that the element with the highest proportion of firms disclosing is CRO assignment (57.6 percent), followed by director

[21] In 2 percent of observations, boards spread CRO responsibility across multiple committees. Therefore, the total committee assignments exceed 100%.

qualifications (40.8 percent), and how senior management engages with the board on cyber-risk matters (20.4 percent). The average disclosure frequencies for all remaining *T-Score* elements range from 0.8 percent (Peer Collaboration) to 9.1 percent (Workforce Cyber Training). Because all firms in my sample report cybersecurity threats as material risk factors, it is surprising that such a large proportion of these firms fail to provide information to stakeholders. Furthermore, I investigate and fail to find evidence suggesting that these firms face meaningful regulatory consequences for remaining silent on these oversight matters.

Table 2, Panel B presents a univariate analysis, comparing mean values for firms that are silent in matters related to cybersecurity oversight (*Cyber_Disclosure* = 0) with those that disclose at least one element of cybersecurity oversight (*Cyber_Disclosure* = 1). I find that, relative to firms that are silent, firms providing stakeholders information about CRO operate in high cyber-risk industries (*High_IndBreach*), are larger (*FirmSize*), have greater holdings by institutional investors (*InstInvest*), have larger boards (*BoardSize*), have boards with directors that serve on three or more boards (*MultiBd_Dir*), have at least one IT expert on the board (*IT_Expert*), and engage Big 4 auditors (*Big4*). This provides univariate evidence of the positive relation between CRO transparency and the level of cyber-risk, stakeholder demand, as well as board resources. I further find that CRO-informative firms are older (*FirmAge*), more profitable (*ROA, Loss*), have higher growth (*Growth*), more leverage (*Leverage*), lower stock returns (*Returns*), lower risk (*MWeak, Lit_Indus*), more complex operations (*Merger*, *Foreign*), as well as more likely to be listed on the NYSE (*NYSE*), as compared to those firms that are silent. Table 2, Panel C presents pairwise correlations, revealing positive univariate correlations between overall transparency, *T-Score*, and all variables of interest in model (1), providing initial support that the level of cyber-risk, demand for board oversight disclosure, as well as the quantity and

nature of board resources are associated with higher levels of board oversight disclosure. Untabulated, variance inflation factors (VIFs) for all test and control variables do not exceed 3.1, suggesting that multicollinearity is not a concern.

Section 5. Empirical Results

5.1. Main Results

To examine firm transparency of board oversight, I first estimate Model (1) using four different oversight disclosure outcomes and present the results in Table 3. In Column (1), I examine the factors associated with a firm's decision to disclose to what board party is CRO assigned (*Discl_Assign*). I find that firms operating in high-cyber-risk industries (*High_IndBreach*, $p < 0.01$) are more likely to disclose CRO assignment, as compared to those firms operating in low-cyber-risk industries. Consistent with my predictions, I find that larger firms (*FirmSize,* $p < 0.01$) and firms with a higher proportion of shares held by institutional investors *(InstInvest,* $p < 0.05$) are more likely to disclose CRO assignment, suggesting the influence of pressure of public visibility and institutional investors promotes oversight disclosure. Finally, I find that board size (*BoardSize,* $p < 0.01$), boards with directors serving concurrently on three or more boards (*MultiBd_Dir,* $p < 0.01$), boards with at least one IT-expert director (*IT_Expert,* $p < 0.01$), and firms using Big 4 auditors (*Big4,* $p < 0.05$) are positively associated with the decision to disclose CRO assignment, suggesting that firms with greater board resources and expertise promote the likelihood of providing oversight information to investors and other market participants.

Related to control variables, I find positive and statistically significant coefficients for firms that are older (*FirmAge,* $p < 0.10$), more profitable (*ROA,* $p < 0.01$), having more leverage (*Leverage,* $p < 0.10$), lower returns (*Returns,* $p < 0.01$), and foreign income (*Foreign,* $p < 0.01$), indicating that such firms are more likely to disclose CRO assignment, as compared to firms without these characteristics. Next, I find a positive relation between the length of the firm's proxy statement filing (*Length*, $p < 0.01$) and the likelihood of disclosing CRO assignment,

suggesting that disclosure decisions around CRO are influenced by the firm's innate overall disclosure strategy. Finally, I find that the area under the Receiver Operating Characteristic (ROC) curve is above the acceptable threshold of 0.70, suggesting that my model has adequate power to predict a firm's choice to provide stakeholders this CRO information.

In Columns (2), (3), and (4), I examine outcomes relating to the decision to disclose board member cybersecurity qualifications (*Discl_Qual*), the reporting process between management and the board on CRO matters (*Discl_Report*), and at least one cybersecurity oversight process or activity (*Discl_Process*) in 2021 proxy statements, respectively. Related to the main variables of interest, I find qualitatively similar results as compared to Column (1) with two exceptions. While firms operating in high-cyber-risk industries remain more likely to disclose how management reports to the board, as well as at least one CRO process or activity (*High_IndBreach*, $p < 0.05$), firms facing high-cyber-risk are *not* likely to disclose director cybersecurity qualifications (*High_IndBreach*, $p > 0.10$).[22] Finally, I do not find that engaging Big 4 auditors is associated with firms providing CRO disclosure relating to director qualifications (*Big4*, $p > 0.10$), nor to CRO processes or activities (*Big4*, $p > 0.10$). Because current SEC regulation requires that, for material risks, firms provide investors information relating to the nature of the board's role in risk oversight, as well as information on how management reports to the board on these matters, these results suggest that Big 4 auditors are influential in the decision to disclose the elements most closely correspond with current SEC

[22] In untabulated analyses, I consider the sensitivity of *High_IndBreach*, which measures the *proportion of firms* reporting a data breach in the prior 3 years, by using a lookback period of 2- and 1-year, and all inferences for predicting outcomes related to *Discl_Assign*, *Discl_Qual*, *Discl_Report*, *Discl_Process*, and *T-Score* remain unchanged. I also repeat these main analyses, replacing *High_IndBreach* with *High_NumBreachInd*, which measures the *number of breaches* reported by industry-peer firms, scaled by the number of peer firms, using lookback periods of 3-, 2-, and 1-year. All inferences are unchanged with one exception. In the decision to disclose director CRO qualifications, I find a positive association with both *High_NumBreachInd* and *Big4*, whereas in the main analyses, the results suggest that there is no association.

regulation (i.e., assignment and reporting), as opposed to increasing overall CRO transparency. Altogether, these results provide additional support that firm characteristics relating to level of cybersecurity risk, demand for cybersecurity disclosure, as well as board resources promote transparency in board oversight of this area of growing risk.

To determine the economic magnitude of the logit coefficients, I calculate the marginal effects of each determinant, while holding all other variables at their means, and find that the likelihood of a firm disclosing CRO assignment increases 4 percent for firms operating in high-cybersecurity-risk industries (*High_IndBreach*, $p < 0.01$), 9 percent for firms with an IT-expert director on the board (*IT_Expert*, $p < 0.01$), and 5 percent for firms engaging Big 4 auditors (*Big4*, $p < 0.01$), suggesting that, while these effects are statistically significant, they are not large effects. I further find that, for continuous variables, moving from the 1st to 3rd quartile while holding all other variables at their means, is estimated to increase the likelihood of CRO assignment disclosure by 32 percent (*FirmSize,* $p < 0.01$), 8.4 percent (*InstInvest,* $p < 0.05$), 16 percent (*BoardSize,* $p < 0.01$), and 8.5 percent (*MultiBd_Dir,* $p < 0.01$). While all the determinants are positive and statistically different from zero, the factors of firm size and the number of directors on the board are the most *economically* significant factors in this disclosure decision. I further consider the marginal effects of each determinant for columns (2), (3), and (4), and find qualitatively similar results. The two factors with the greatest economic significance continue to be firm size (*FirmSize* coeff. = 17.5, 17.4, and 20.9, respectively), and board size (*BoardSize* coeff. = 21.3, 42.2, and 21.3, respectively). However, holdings by institutional investors also greatly influence these disclosure decisions (*InstInvest* coeff. 17.1, 14.7, and 14.1, respectively). Altogether, the evidence suggests that these determinants influence a firm's decision to provide board oversight information to stakeholders.

Next, I consider factors influencing *the extent to which* a firm is transparent about its board oversight practices. I replace the dependent variable, *Disclose_CRO,* in Model (1) with *T-Score*, which measures the number of CRO program elements disclosed in a firm's proxy statement, and ranges from 0 to 12. Table 4 presents the results. In column (1), I examine the influence of cybersecurity risk, stakeholder demand for disclosure, and board resources on CRO disclosure (*T-Score*) and find qualitatively similar results as those found in Table 3, although the use of Big4 auditors (*Big4*, $p > 0.10$) is no longer associated with CRO disclosure. In column (2), I consider whether *the nature of* CRO assignment influences disclosure decisions, relative to those firms that are silent on CRO assignment. I add three indicator variables to the model: 1) for firms that fully retain CRO responsibility at the board level (*CRO_BoardOnly*), 2) those that fully delegate CRO responsibility to a committee (*CRO_CommOnly*), and 3) those that share CRO responsibility between the full board and a named committee (*CRO_Shared*). I make no predictions relating to the influence the nature of CRO assignment on disclosure decisions.

I find positive coefficients on all three CRO assignment variables, which is expected mechanically. When I perform an F-test for equality of coefficients between the pairs of different assignment types, I find that firms that share CRO responsibility between the full board and a committee have greater overall disclosure, as compared to those boards that fully retain CRO responsibility, as well as those boards that fully delegate CRO to a specified committee (F-statistic equal to 49.70 and 92.09, respectively). Shared responsibility commits the greatest quantity of board resource to oversight efforts, including a breadth (e.g., all board members), as well as depth (e.g., a committee with special focus). Furthermore, according to Larcker and Tayan (2020), the best practice for risk management is a broad approach utilizing the full board, and leveraging committees when the area of risk requires specialized skills and knowledge, as is

the case with cyber-risk. Therefore, shared responsibility for oversight of cybersecurity risk may reflect an overall higher quality governance structure at these firms.

Finally, in Column (3), I use a reduced sample of those firms that disclose how CRO is allocated across the board, and examine whether the *choice of committee* tasked with CRO influences the extent to which a firm discloses CRO elements. I add indicator variables for those firms that assign CRO to the audit committee (*CRO_Audit*), the risk committee (*CRO_Risk*), to the technology committee (*CRO_Tech*), and to other named committees (*CRO_Other*). I make no predictions relating to the influence of committee assignment on disclosure decisions. Relative to firms where the full board retains CRO responsibility, I find that firms where CRO is assigned to the risk committee provide greater cybersecurity disclosure (*CRO_Risk*, $p < 0.05$). [23] Altogether, the results of columns (2) and (3) suggest that risk oversight assignment is an influential factor in disclosure decisions, and that greater resource (i.e., having *both* full board and a committee with a specialized focus), or a risk-focused committee (as compared to overburdened audit committees), increase the level of information provided to stakeholders.

Sensitivity Tests

I conduct two separate sensitivity tests of the analyses that uses *T-Score* to measure the extent of CRO transparency. First, I consider whether the results are sensitive to the characterization of *T-Score*, using two modified versions that reduce the influence of outliers. I create *T-Score_b*, which limits *T-Score* to elements #1 through #3: the assignment of cybersecurity oversight, director cybersecurity qualifications, and information relating to how management reports to the board on cybersecurity matters, and ranges from zero to three. These

[23] I recognize that CRO assignment to a risk committee is conditional on a board *having formed* a separate risk committee, which is not a regulatory requirement for firms. Therefore, in additional analysis, I examine cross-sectionally how factors influencing CRO disclosure vary depending on whether a board has elected to form a risk committee.

three elements most closely align with items that are more-explicitly identified in current and proposed SEC disclosure rules. Next, I create *T-Score_c*, which ranges from zero to four, and is constructed using *T-Score_b*, plus the maximum of *T-Score* elements #4 through #12, which include individual processes used to oversee cybersecurity risk, and are items that the SEC more generally "encourages" firms to disclose to stakeholders. Using these alternate T-Scores, I reperform analyses reported in Table 4. Untabulated, all inferences are unchanged with one exception. For both *T-Score_b* and *T-Score_c*, when analyzing the influence of different committee assignments on CRO disclosure, I find that, in addition to the positive association between levels of disclosure and risk committees CRO assignments, I similarly find a positive association for firms where CRO is assigned to technology committees, as compared to firms where the board retains full responsibility.

Second, I use principal component analysis (PCA) to reduce the 12 elements to extract a composite *T-Score* measure of the 12 elements. I find that the first principal component, which I label *pc_T-Score*, has an eigenvalue greater than one and explains 27 percent of the variance (untabulated). I then use *pc_T-Score* to re-examine the main model. I also consider whether the PCA results are sensitive to the characterization of *T-Score*. I similarly create *pc_T-Score_b* and *pc_T-Score_c* using the first principal component of each measure and rerun my main tests using these alternative dependent variables. Untabulated, the inferences from these tests, using the first component for all three measures of *T-Score*, remain unchanged.

5.2. Additional Analyses

Cross-Sectional Analysis: Firms with and without Risk Committees

Boards have flexibility in deciding how to allocate its oversight and advisory responsibilities across the full board and its various committees. While some boards approach

risk oversight comprehensively and retain responsibility at the board level, others often choose to delegate risk oversight to the audit committee, which already has primary responsibility for overseeing financial reporting risks. Although not required, a smaller proportion of boards choose to form separate risk committees. According to Larcker and Tayan (2020), there are factors relating to when a board will likely benefit from forming a separate risk committee: when the audit committee is otherwise overburdened by regulatory requirements, or when the nature of the risk is operational or requires specialized knowledge. In such cases, members of a separate risk committee can dedicate time and provide necessary expertise to effectively oversee the risk.

Because firms that have separate risk committees may be fundamentally different than those firms that do not, I separately examine the determinants of CRO disclosure for the two types of firms. Using the full sample, I regress *T-Score* on the independent variables in Model (1) and present the results in Table 5. Columns (1) and (2) report the results for firms that have separate risk committees and those that do not, respectively. Untabulated, only 12.6 percent of firms in my sample have separate risk committees. I find that the main effects are concentrated in firms that do not form separate risk committees. Specifically, I find that, while many of the determinants promote higher amounts of information disclosure, for boards that have elected to form a risk committee, there is no longer an association between high cybersecurity risk (*High_IndBreach*, $p > 0.10$) and CRO disclosure. I further find mixed results relating to stakeholder demand for information. Specifically, I find that institutional investors influence those firms with risk committees (*InstInvest*, $p < 0.01$), whereas firm size (*FirmSize*, $p < 0.01$) is influential for only firms without risk committees. Finally, I find that boards with directors sitting on three or more boards concurrently (*MultiBd_Dir*, $p < 0.01$) provide greater information

transparency only in firms without separate risk committees, suggesting that the increase in exposure to other boards' approach to CRO positively impacts firm transparency.

Cross-Sectional Analysis: Breached versus Non-Breached Firms

Firms that have previously reported a data breach may be motivated to provide stakeholders comfort that the breach is not an ex post indicator of weak controls at the firm (Lawrence et al. 2018). Therefore, breach-reporting firms have incentive to provide stakeholders more thorough disclosure about cybersecurity measures, as well as board oversight of these efforts, that will prevent future incidents. However, prior research reports a lack of meaningful consequences for individual firms that report data breaches, finding no impact on future financial performance, audit fees, material internal control weaknesses, and only minimal negative short-window returns, which disappear a few days after the reported breach (Richardson et al. 2019). Furthermore, it is rare for the SEC, during its filing review process, to issue comment letters relating to cybersecurity disclosure. Therefore, it is unclear whether previously breached firms will provide stakeholders different levels of CRO information than non-breached firms.

Table 5, Columns (3) and (4) report the results for those firms that have, and have not, reported a data breach in the three years prior to their 2021 DEF 14A filing, respectively. Untabulated, I find that 8 percent of firms in my sample have reported a data breach. I further find that higher cybersecurity risk, stakeholder demand, and board resources continue to be influential in non-breached firms. However, I fail to find evidence that institutional investors (*InstInvest*, $p > 0.10$) and larger boards (*BoardSize*, $p > 0.10$) influence disclosure decisions for breached firms. As was the case for firms with and without separate risk committees, I find no evidence for either breached or non-breached firms that engaging Big 4 auditors (*Big4*, $p > 0.10$) is associated with CRO disclosure.

Industry Analysis

My main tests examine the likelihood of a firm disclosing different types and levels of information relating to their oversight of cybersecurity, on average. However, cybersecurity disclosure decisions likely vary depending on the industry in which the firm operates. I do not include industry fixed effects in my main analyses because, when included in the model, the variance inflation factors (VIFs) exceed ten, indicating that high correlation among model variables is cause for concern. Instead, I include *High_IndBreach* to examine whether firms operating in industries facing high cybersecurity risk are likely to provide greater transparency in CRO matters, and find supporting evidence. Because industries have varying levels of exposure to breaches, based on the quantity and sensitivity of the information stored, and because peer disclosure spillover can happen amongst similar firms, it is important to understand how a firm's industry impacts the amount of CRO information they provide to stakeholders.

First, I examine, the frequency of each *T-Score* element disclosed by industry sectors, using the Fama-French 12 industry classification. The results are presented in Table 6. The table is conditionally formatted using greyscale coloring, such that the darker (lighter) the shading, the higher (lower) the disclosure frequency for each *T-Score* element, as compared across industry sectors. I find that, on average, firms in the healthcare industry (FF-10) provide the lowest overall level of CRO information, disclosing 0.90 *T-Score* elements. This is consistent with a recent Moody's Investor Services press release that, while critical and sensitive information is stored by healthcare firms, these firms are among the least transparent in cyber risk mitigation strategies (Moody's Investor Service 2019). I further find that utility firms (FF-8) provide the highest level of transparency, disclosing 2.54 elements, respectively, and that two *T-Score* elements are disclosed at a frequency more than double the average firm: workforce cyber

training and peer collaboration. I further find that technology-centric firms (FF-6) are more nearly three-times as likely to disclose executive cybersecurity expertise, which may be a reflection of the executive team composition, while those firms in the telecom industry (FF-7) are more than twice as likely to tie cybersecurity performance to executive compensation. Interestingly, financial institutions (FF-11), which are deemed to be more highly exposed to cybersecurity risk due to the nature and extent of stored information, appear to be neither high- nor low-frequency disclosers for any of the *T-Score* elements.

Finally, despite the suspected multicollinearity issues, I examine whether cybersecurity risk, stakeholder demand, and board resources continue to be influential in the level of transparency, holding constant the industry in which a firm operates. I rerun the main tests, adding industry fixed effects (Fama-French 12). Untabulated, when I separately examine the likelihood of a firm to disclose CRO assignment, director qualifications, reporting from management to the board, or at least one CRO process, I find qualitatively similar results with one exception. I no longer find an association between firms operating in high-risk industries and the propensity to disclose any of these items. When I examine the extent to which a firm is transparent regarding CRO information, again I find no association for firms in high-risk industries, while all other inferences remain the same (untabulated). In both analyses, because of high collinearity between *High_IndBreach* and one or more of the industry fixed effects dummy variables, these issues may be driving the null result. Therefore, I cautiously interpret these tests as supporting the main results, albeit with weak support for firms operating in high-cyber-risk industries.

Ex Ante Measures of Cybersecurity Risk

I recognize that the industry variable I construct for the main analyses is an ex-post measure that identifies high-cyber-risk industries using past breach incident data. Therefore, I next consider *ex-ante* measures of cyber-risk related to industry classification, as well as other factors, to determine the impact of each on CRO transparency. Moody's Investor Service, which is cited in the SEC's proposed cybersecurity disclosure rules, names the two most exposed sectors to cybersecurity risk as financial institutions and healthcare service providers, due to the detailed and sensitive nature of the data stored by these entities (Moody's Investor Service 2019). Therefore, I replace *High_IndBreach* with *HighRiskInd*, an indicator equal to one for financial firms or healthcare service providers (a subset of the larger healthcare industry), and zero otherwise. Untabulated, I find that firms operating in high-cyber-risk industries provide more CRO information to stakeholders (coeff. = 0.345, p-value < 0.01), as compared to those that are not. Next, I separately examine financial firms and healthcare service providers and find that the effect is limited to financial firms. However, because there are only 37 healthcare service firms in my sample, this may be due to lack of power. In both analyses, with the exception of *Big4* auditors, the coefficients of the determinants relating to stakeholder demand and board resources continue to be positive.

The next two ex-ante measures focus on existing control variables that represent factors known to increase computer network vulnerability to hacker activity. First, hackers often target firms that have recently completed a merger or acquisition (*Merger*) because of the increased vulnerability while firms migrate data and merge IT systems (Lee 2022). Next, global firms (*Foreign*), with disbursed computer infrastructure, production networks, and supply chains, provide widespread business disruption opportunities for hackers (Allianz 2022). Because these

factors are independent of firm industry, I rerun model (1), dropping the proxy for high-cyber-risk industry while adding industry fixed effects. Untabulated, I find that the coefficient on *Merger* is not different from zero (p-value > 0.10), whereas the coefficient on *Foreign* is positive (coeff. = 0.186, p-value < 0.01). All other included determinants relating to stakeholder demand and board resources continue to be associated with greater CRO transparency.

Overall, these results suggest that firm characteristics relating to the level of cybersecurity risk, stakeholder demand for CRO disclosure, and board resources promote the likelihood of, and the extent to which, a firm provides transparency of board oversight to market participants. Furthermore, the findings in my study suggest that there is a dearth of information relating to cybersecurity oversight, making it difficult for market participants to accurately gauge cyber risk, to make informed investment decisions, and to hold directors accountable. This is consistent with the motivation behind the SEC's current rulemaking release, which seeks to standardize disclosure around cybersecurity risk management and governance.

Section 6. Conclusion

Cybersecurity disclosure is an important mechanism for firms to provide information that allows stakeholders to assess a firm's posture and readiness, given increasing frequency and severity of data security breaches. It is important to understand how boards are fulfilling their oversight responsibilities and, importantly, how they inform market participants of those activities. The SEC's recently proposed cybersecurity disclosure rules, and the general support found in comment letters received, suggest that this continues to be an area of critical importance to stakeholders. In this study, I use a sample of 2,921 proxy statements filed in 2021 to examine the factors that promote the extent to which a firm is provides information about its risk oversight responsibilities related to cybersecurity.

I find that nearly 58 percent of firms in my sample disclose how CRO is allocated across the board, including 10 percent that retain CRO responsibility at the board level, 27 percent of boards delegate the responsibility to a committee, and 20 percent of boards share the responsibility between the full board and a specified committee. Relating to committee assignments, the audit committee is most frequently charged with CRO responsibility (77%). After controlling for underlying firm characteristics, I find that, on average, the level of cybersecurity risk facing a firm, the amount of stakeholder demand for disclosure, as well as board resources are positively associated with a firm's decision to provide CRO information to stakeholders. Although Big 4 auditors, which advise clients in disclosure decisions, are typically associated with higher quality disclosure, I find only limited evidence that the use of Big 4 auditors is positively associated with firm transparency in cybersecurity oversight matters. All inferences are robust to alternate measures of *T-Score*, analysis using principal component analysis, as well as the inclusion of industry fixed effects.

When examining whether the party to whom CRO is assigned impacts disclosure decisions, I find that firms that share oversight responsibility between the full board and a specified committee provide higher levels of transparency, as compared to those firms that assign CRO to *either* the full board or a committee. I further find that boards delegating responsibility to a separate risk committee are more transparent, relative to those boards that delegate CRO to audit, technology, or another specified committee. In cross-sectional analyses, I find that the influence of these determinants is generally stronger for firms without separate risk committees, as well as for firms that have not previously reported a breach. Finally, I find that the influence of holdings by institutional investors is present only in firms with separate risk committees and for non-breached firms.

This study extends prior literature examining cybersecurity risk factor disclosures by examining the determinants of disclosure relating to the governance over those risks. It further provides important descriptive information in disclosure quality an area of heightened investor interest and regulatory scrutiny. Because my study precedes proposed SEC cybersecurity disclosure rule changes, these findings provide a better signal to market participants regarding governance quality. Finally, my study provides a valuable baseline for future research examining whether, and to what extent, the new SEC cybersecurity disclosure rules have on firm disclosure decisions, as well as other cybersecurity-related outcomes. There is one important limitation to this study worth noting. Because smaller reporting companies are not required to include Item 1A Risk Factors in their annual reports, and because I only include in my sample firms that report material cyber-related risks in their annual reports, the results in this study may not

generalize to firms electing to prepare their financial statements in accordance with the smaller reporting company rules.[24]

[24] As of June 28, 2018, SEC defines "smaller reporting company" as a firm that has a public float of less than $250 million, or if it has less than $100 million in annual revenue and 1) no public float, or 2) public float of less than $700 million. For additional information, see https://www.sec.gov/education/smallbusiness/goingpublic/SRC. For the reporting rules applicable to smaller reporting companies, see https://www.ecfr.gov/current/title-17/chapter-II/part-210/subject-group-ECFR9da2cb911847a61.

References

Allianz. 2022. *Allianz Risk Barometer*. http://www.agcs.allianz.com/assets/PDFs/Reports/AllianzRiskBarometerTopBusinessRisks2016.pdf

Amir, E., Levi, S., and Livne, T. 2018. Do Firms Underreport Information on Cyber-Attacks? Evidence from Capital Markets. *Review of Accounting Studies*, *23*, 1177–1206. https://doi.org/https://doi.org/10.1007/s11142-018-9452-4

Ashraf, M., Michas, P. N., and Russomanno, D. 2020. The Impact of Audit Committee Information Technology Expertise on the Reliability and Timeliness of Financial Reporting. *Accounting Review*, *95*(5), 23–56. https://doi.org/10.2308/ACCR-52622

Bochkay, K., Choi, S., and Hales, J. 2022. 'Mere Puffery' or Credible Disclosure? The Real Effects of Adopting Voluntary ESG Disclosure Standards. *Working Paper*.

Brooks, C. 2021. Alarming Cybersecurity Stats: What You Need To Know For 2021. *Forbes*, 1–10. https://www.forbes.com/sites/chuckbrooks/2021/03/02/alarming-cybersecurity-stats----------what-you-need-to-know-for-2021/?

Brown, S. V., Tian, X. (Shaolee), and Wu Tucker, J. 2018. The Spillover Effect of SEC Comment Letters on Qualitative Corporate Disclosure: Evidence from the Risk Factor Disclosure. *Contemporary Accounting Research*, *35*(2), 622–656. https://doi.org/10.1111/1911-3846.12414

Canales, K., and Jibilian, I. 2021. The US is Readying Sanctions Against Russia over the SolarWinds Cyber Attack. Here's a Simple Explanation of How the Massive Hack Happened and Why It's Such a Big Deal. *Business Insider*. https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12?r=US&IR=T

Coles, J. L., Daniel, N. D., and Naveen, L. 2008. Boards: Does One Size Fit All? *Journal of Financial Economics*, *87*(2), 329–356. https://doi.org/10.1016/j.jfineco.2006.08.008

Cunningham, L. M., and Leidner, J. J. 2022. The SEC Filing Review Process: A Survey and Future Research Opportunities†. *Contemporary Accounting Research*, *39*(3), 1654–1688. https://doi.org/10.1111/1911-3846.12742

DeFond, M., and Zhang, J. 2014. A Review of Archival Auditing Research. *Journal of Accounting and Economics*, *58*, 275–326. https://doi.org/10.1016/j.jacceco.2014.09.002

Deloitte. 2021. *2021 Future of Cyber Survey*. https://www2.deloitte.com/us/en/pages/advisory/articles/future-of-cyber-survey.html

Dhaliwal, D. S., Kaplan, S. E., Laux, R. C., and Weisbrod, E. 2013. The Information Content of Tax Expense for Firms Reporting Losses. *Journal of Accounting Research*, *51*(1), 135–164. https://doi.org/10.1111/j.1475-679X.2012.00466.x

Dunn, K. A., and Mayhew, B. W. 2004. Audit Firm Industry Specialization and Client Disclosure Quality. *Review of Accounting Studies*, *9*, 35–58. https://doi.org/10.1023/B:RAST.0000013628.49401.69

Eaton, C., and Volz, D. 2021. Colonial Pipeline CEO Tells Why He Paid Hackers a $4.4 Million Ransom. *The Wall Street Journal*. https://www.wsj.com/articles/colonial-pipeline-ceo-tells-why-he-paid-hackers-a-4-4-million-ransom-11621435636

EY. 2021. Cybersecurity: How Do You Rise Above the Waves of a Perfect Storm? *EY Global Information Security Survey 2021*. https://www.ey.com/en_us/cybersecurity/cybersecurity-how-do-you-rise-above-the-waves-of-a-perfect-storm

Fama, E. 1980. Agency Problems and the Theory of the Firm. *The Journal of Political Economy*,

88(2), 288–307. https://doi.org/10.1017/CBO9780511817410.022
Farrell, K. A., and Whidbee, D. A. 2002. Monitoring by the Financial Press and Forced CEO Turnover. *Journal of Banking and Finance*, *26*, 2249–2276. https://doi.org/10.1016/S0378-4266(01)00183-2
Federal Bureau of Investigation (FBI). 2021. *Internet Crime Report 2021*. https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf
Federal Trade Commission (FTC). 2019. *Equifax to Pay $575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach*. https://www.ftc.gov/news-events/news/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related-2017-data-breach
Francis, J., Philbrick, D., and Schipper, K. 1994. Shareholder Litigation and Corporate Disclosures. *Journal of Accounting Research*, *32*(2), 137. https://doi.org/10.2307/2491279
Gaulin, M. 2017. Risk Fact or Fiction: The Information Content of Risk Factor Disclosures. *Dissertation - Rice University*, *March*, 1–102.
Gensler, G. 2022. *Remarks on Cybersecurity and Securities Laws at the Northwestern University Pritzker School of Law*. https://www.sec.gov/news/speech/gensler-cybersecurity-and-securities-laws-20220124
Gordon, L. A., Loeb, M. P., Lucyshyn, W., and Sohail, T. 2006. The Impact of the Sarbanes-Oxley Act on the Corporate Disclosures of Information Security Activities. *Journal of Accounting and Public Policy*, *25*(5), 503–530. https://doi.org/10.1016/j.jaccpubpol.2006.07.005
Gordon, L. A., Loeb, M. P., and Sohail, T. 2010. Market Value of Voluntary Disclosures Concerning Information Security. *MIS Quarterly*, *34*(3), 567–594. https://doi.org/https://doi.org/10.2307/25750692
Guernsey, S., Gao, F., Liu, T., and Serfling, M. 2022. Classified Boards: Endangered Species or Hiding in Plain Sight. *Working Paper*.
Healy, P. M., and Palepu, K. G. 2001. Information Asymmetry, Corporate Disclosure, and the Capital Markets: A Review of the Empirical Disclosure Literature. *Journal of Accounting and Economics*, *31*, 405–440. https://doi.org/10.1016/S0165-4101(01)00018-0
Hermalin, B. E., and Weisbach, M. S. 2012. Information Disclosure and Corporate Governance. *Journal of Finance*, *67*(1), 195–233. https://doi.org/10.1111/j.1540-6261.2011.01710.x
Héroux, S., and Fortin, A. 2020. Cybersecurity Disclosure by the Companies on the S&P/TSX 60 Index. *Accounting Perspectives*, *19*(2), 73–100. https://doi.org/10.1111/1911-3838.12220
Higgs, J. L., Pinsker, R. E., Smith, T. J., and Young, G. R. 2016. The Relationship Between Board-Level Technology Committees and Reported Security Breaches. *Journal of Information Systems*, *30*(3), 79–98. https://doi.org/10.2308/isys-51402
Hoberg, G., and Phillips, G. 2010. Product Market Synergies and Competition in Mergers and acquisitions: A Text-Based Analysis. *Review of Financial Studies*, *23*(10), 3773–3811. https://doi.org/10.1093/rfs/hhq053
Hoberg, G., and Phillips, G. 2016. Text-Based Network Industries and Endogenous Product Differentiation. *Journal of Political Economy*, *124*(5), 1423–1465. https://doi.org/10.1086/688176
Iliev, P., Kalodimos, J., and Lowry, M. 2021. Investors' Attention to Corporate Governance. *Review of Financial Studies*, *34*(12), 5581–5628. https://doi.org/10.1093/rfs/hhab003
Jeong, C. Y., Lee, S. T., and Lim, J. 2019. Information Security Breaches and IT Security

Investments: Impacts on Competitors. *Information & Management*, *56*, 681–695. https://doi.org/10.1016/j.im.2018.11.003
Jiang, W., Legoria, J., Reichelt, K., and Walton, S. 2022. Firm Use of Cybersecurity Risk Disclosure. *Journal of Information Systems*, *36*(1), 151–180. https://doi.org/https://doi.org/10.2308/ISYS-2020-067
Kashmiri, S., Nicol, C. D., and Hsu, L. 2017. Birds of a Feather: Intra-industry Spillover of the Target Customer Data Breach and the Shielding Role of IT, Marketing, and CSR. *Journal of the Academy of Marketing Science*, *45*, 208–228. https://doi.org/10.1007/s11747-016-0486-5
Lankton, N., Price, J. B., and Karim, M. 2021. Cybersecurity Breaches and the Role of Information Technology Governance in Audit Committee Charters. *Journal of Information Systems*, *35*(1), 101–119. https://doi.org/10.2308/isys-18-071
Larcker, D. F., and Tayan, B. 2020. *Corporate Governance Matters: A Closer Look at Organizational Choices and Their Consequences 3rd Edition*.
Lawrence, A., Minutti-Meza, M., and Vyas, D. 2018. Is Operational Control Risk Informative of Financial Reporting Deficiencies? *AUDITING: A Journal of Practice & Theory*, *37*(1), 139–165. https://doi.org/10.2308/ajpt-51784
Lee, F. 2022. Cybersecurity Risks Pose 'Significant Threat' to Merger Process, New Data Shows. *Agenda*.
Lending, C., Minnick, K., and Schorno, P. J. 2018. Corporate Governance, Social Responsibility, and Data Breaches. *The Financial Review*, *53*, 413–455. https://doi.org/10.1111/fire.12160
Leuz, C., and Wysocki, P. D. 2016. The Economics of Disclosure and Financial Reporting Regulation: Evidence and Suggestions for Future Research. *Journal of Accounting Research*, *54*(2), 525–622. https://doi.org/10.1111/1475-679X.12115
Li, H., No, W. G., and Wang, T. 2018. SEC's Cybersecurity Disclosure Guidance and Disclosed Cybersecurity Risk Factors. *International Journal of Accounting Information Systems*, *30*(June), 40–55. https://doi.org/10.1016/j.accinf.2018.06.003
Martin, K. D., Borah, A., and Palmatier, R. W. 2017. Data Privacy: Effects on Customer and Firm Performance. *Journal of Marketing*, *81*(January), 36–58. https://doi.org/10.1509/jm.15.0497
McPhillips, S., and Osea, S. 2021. QualityScore: Methodology. *Harvard Law School Forum on Corporate Governance*. https://corpgov.law.harvard.edu/2021/02/25/qualityscore-methodology-guide/
Miller, M. 2020. FBI Sees Spike in Cyber Crime Reports During Coronavirus Pandemic. *The Hill*. https://thehill.com/policy/cybersecurity/493198-fbi-sees-spike-in-cyber-crime-reports-during-coronavirus-pandemic/
Moody's Investor Service. 2019. *Cybersecurity Disclosures Vary Greatly in High-Risk Industries*. https://www.moodys.com/research/Moodys-Cybersecurity-disclosures-vary-greatly-in-high-risk-industries--PBC_1196854
Mueller, R. S. 2012. Combating Threats in the Cyber World: Outsmarting Terrorists, Hackers, and Spies. *Speech given at the RSA Cyber Security Conference*. https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies
Munter, P. 2021. *Statement on OCA's Continued Focus on High Quality Financial Reporting in a Complex Environment*. https://www.sec.gov/news/statement/munter-oca-2021-12-06
National Association of Corporate Directors (NACD), Internet Security Alliance, and World

Economic Forum. 2021. *Principles for Board Governance of Cyber Risk*. https://www3.weforum.org/docs/WEF_Cyber_Risk_Corporate_Governance_2021.pdf
New York Stock Exchange (NYSE). 2014. *NYSE: Corporate Governance Guide*. https://www.nyse.com/publicdocs/nyse/listing/NYSE_Corporate_Governance_Guide.pdf
Nicodemus, A. 2022. Gensler Says SEC to Consider New Rules for Cybersecurity, Data Privacy Disclosures. *Compliance Week*. https://www.complianceweek.com/regulatory-policy/gensler-says-sec-to-consider-new-rules-for-cybersecurity-data-privacy-disclosures/31283.article
Perols, R. R., and Murthy, U. S. 2021. The Impact of Cybersecurity Risk Management Examinations and Cybersecurity Incidents on Investor Perceptions and Decisions. *AUDITING: A Journal of Practice & Theory*, *40*(1), 73–89. https://doi.org/10.2308/AJPT-18-010
Poulsen, K., Mcmillan, R., and Volz, D. 2020. SolarWinds Hack Victims: From Tech Companies to a Hospital and University. *Wall Street Journal*. https://www.wsj.com/articles/solarwinds-hack-victims-from-tech-companies-to-a-hospital-and-university-11608548402
PwC. 2022. *2022 Global Digital Trust Insights Survey*. https://www.pwc.com/gx/en/issues/cybersecurity/global-digital-trust-insights.html
RavenPack News Analytics. 2016. *User Guide and Service Overview for WRDS Users*. https://www.ravenpack.com/products/edge/data/news-analytics
Richardson, V. J., Smith, R. E., and Watson, M. W. 2019. Much Ado about Nothing: The (Lack of) Economic Impact of Data Privacy Breaches. *Journal of Information Systems*, *33*(3), 227–265. https://doi.org/10.2308/isys-52379
Schneider, A., and Arnold, C. 2019. Equifax to Pay up to $700 Million in Data Breach Settlement. *NPR*. hhttps://www.npr.org/2019/07/22/744050565/equifax-to-pay-up-to-700-million-in-data-breach-settlement
Smaili, N., Radu, C., and Khalili, A. 2022. Board Effectiveness and Cybersecurity Disclosure. *Journal of Management and Governance*, 1–23. https://doi.org/https://doi.org/10.1007/s10997-022-09637-6
Steinbart, P. J., Raschke, R. L., Gal, G., and Dilla, W. N. 2012. The Relationship Between Internal Audit and Information Security: An Exploratory Investigation. *International Journal of Accounting Information Systems*, *13*(3), 228–243. https://doi.org/10.1016/j.accinf.2012.06.007
Temple-Raston, D. 2021. A "Worst Nightmare" Cyberattack: The Untold Story of the SolarWinds Hack. *Npr*. https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack
U.S. Securities and Exchange Commission (SEC). 1975. *17 CFR § 229.105 - (Item 105) Risk factors*. https://www.law.cornell.edu/cfr/text/17/229.407
U.S. Securities and Exchange Commission (SEC). 2009. *Final Rule: Proxy Disclosure Enhancements*. https://doi.org/10.1007/978-90-6704-437-0_7
U.S. Securities and Exchange Commission (SEC). 2011. *Division of Corporation Finance - Disclosure Guidance: Topic No. 2: Cybersecurity*. https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm
U.S. Securities and Exchange Commission (SEC). 2018. *Commission Statement and Guidance on Public Company Cybersecurity Disclosures*. https://www.sec.gov/rules/interp/2018/33-10459.pdf
U.S. Securities and Exchange Commission (SEC). 2022a. *Press Release: SEC Proposes Rules on*

Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies. https://www.sec.gov/rules/proposed/2022/33-11038.pdf

U.S. Securities and Exchange Commission (SEC). 2022b. *Proposed rule: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure*. https://www.sec.gov/rules/proposed/2022/33-11038.pdf

U.S. Securities and Exchange Commission (SEC). 2022c. *SEC Reopens Comment Periods for Several Rulemaking Releases Due to Technological Error in Receiving Certain Comments*.

Vincent, N. E., Higgs, J. L., and Pinsker, R. E. 2019. Board and Management-Level Factors Affecting the Maturity of IT Risk Management Practices. *Journal of Information Systems*, *33*(3), 117–135. https://doi.org/10.2308/isys-52229

Walton, S., Wheeler, P. R., Zhang, Y., and Zhao, X. 2021. An Integrative Review and Analysis of Cybersecurity Research Current State and Future Directions. *Journal of Information Systems*, *35*(1), 155–186. https://doi.org/10.2308/ISYS-19-033

Wang, T., Kannan, K. N., and Ulmer, J. R. 2013. The Association Between the Disclosure and the Realization of Information Security Risk Factors. *Information Systems Research*, *24*(3), 201–218. https://doi.org/https://doi.org/10.1287/isre.1120.0437

White, H. 1980. A Heteroskedasticity-Consistent Covariance Matrix Estimator and a Direct Test for Heteroskedasticity. *Econometrica*, *48*(4), 817–838. https://doi.org/https://doi.org/10.2307/1912934

Whited, R. L., Swanquist, Q. T., Shipman, J. E., and Moon, J. R. 2022. Out of Control: The (Over) Use of Controls in Accounting Research. *The Accounting Review*, *97*(3), 395–413. https://doi.org/https://doi.org/10.2308/TAR-2019-0637

Wickline, H. 2021. Getting Past Hacks and Attacks: The News Media's Deepening Coverage of Cybersecurity Issues. *Hewlett Foundation*. https://hewlett.org/getting-past-hacks-and-attacks-the-news-medias-deepening-coverage-of-cybersecurity-issues/

Appendices

Appendix A: Variable Definitions

Variable Name	Variable Description (Source)
Dependent Variables	
Discl_Assign	An indicator variable equal to one if a firm discloses the assignment for CRO to either the full board, to a committee, or to a combination thereof, and zero otherwise. (Appendix B, #1) (DEF 14A)
Discl_Report	An indicator variable equal to one if the firm how senior management reports to the board on CRO matters (e.g., parties involved, frequency of reports or meetings), and zero otherwise. (Appendix B, #3) (DEF 14A)
Discl_Process	An indicator variable equal to one if a firm discloses at least one CRO process, and zero otherwise. (Appendix B, #4 - 12) (DEF 14A)
T-Score	A discrete number between zero and twelve based on the number of CRO elements disclosed. (Appendix B) (DEF 14A)
Variables of Interest	
High_IndBreach	An indicator variable equal to one if the proportion of industry-peer firms that have reported a data breach in the previous three years is greater than the median, and zero otherwise. To construct the industry peer groups, I use Hoberg-Phillips TNIC peer data, and require that firms have 10 or more peers. For those firms that have fewer than 10 TNIC peers, I next use 4-digit SIC, followed by 3-digit SIC, and finally 2-digit SIC, requiring 10 or more peer firms before moving to the next level of industry classification. (AA, Comp, TNIC)
FirmSize	The natural log of the market value of equity ($PRCC\_F_t$*$CSHO_t$), in millions (Comp)
InstInvest	Percent of outstanding common shares owned by institutional investors (CRSP, TR)
BoardSize	The number of directors on the board (BrdEx)
MultiBd_Dir	The proportion of directors on the board that serve on three or more concurrent boards (BrdEx)

IT_Expert	An indicator variable equal to one if at least one director is an Information Technology (IT) expert, defined as one who is a current or former Chief Information Officer (CIO), or has experience working in IT or cybersecurity (using method similar to Ashraf et al. (2020). See footnote 11 for full list of keyword search terms), and zero otherwise (BrdEx)
Big4	An indicator variable equal to one if the firm is audited by Deloitte, KPMG, Ernst and Young, or PwC, and zero otherwise (Comp)
Control Variables	
FirmAge	The natural log of firm age, calculated as the number of years the firm has been included in Compustat (Comp)
ROA	Income before extraordinary items (IB) scaled by lagged total assets (AT_{t-1}) (Comp)
Growth	The market to book ratio ($PRCC\_F_t$*$CSHO_t$)/(CEQ_t) (Comp)
Leverage	The sum of total long-term debt ($DLTT_t$) and total current liabilities (DLC_t), scaled by total assets (AT_t) (Comp)
Loss	An indicator variable equal to one if the firm has negative net income (IB), and zero otherwise (Comp)
Returns	The buy-and-hold returns for the prior 12 months, less buy-and-hold annual returns for the value-weighted portfolio (CRSP)
MWeak	An indicator variable equal to one if the internal control opinion (under SOX section 404) is a qualified opinion for a material weakness in the prior year, and zero otherwise (AA)
Lit_Indus	An indicator equal to one if the firm operates in SICH 2833 – 2836, 3570 – 3577, 3600 – 3674, 5200 – 5961, 7370 – 7374, or 8731 – 8734, following Francis et al. (1994), and zero otherwise (Comp)
Merger	An indicator variable equal to one if firm engaged in a merger or acquisition (AQP), and zero otherwise (Comp)
Foreign	An indicator equal to one if the firm has pre-tax foreign income or loss (PIFO), and zero otherwise (Comp)
NYSE	An indicator variable equal to one if the firm is listed on the NYSE index (EXCHG #11), and zero otherwise (Comp)
Length	The natural log of the word count for a firm's most recent proxy statement (SEC)

Notes: 'AA' refers to Audit Analytics, 'BrdEx' to BoardEx, 'Comp' to Compustat Fundamentals Annual, and 'CRSP' to The Center for Research in Security Prices, LLC (CRSP), "DEF 14A" to a firm's 2021 proxy filing, "SEC" to SEC Analytics Suite by WRDS, and 'TNIC' to Hoberg-Phillips TNIC data, and 'TR' to Thomson Reuters Institutional (13f) Holdings.

Appendix B: Transparency Score (*T-Score*) Elements Descriptions and Examples

The following provides background information, definitions, as well as examples relating to the 12 risk oversight elements that I identify in proxy filings to measure each firm's Transparency Score (*T-Score*):

1. **The assignment of cybersecurity oversight**
   a. Background: CRO can be the responsibility of the board-at-large, a committee, a combination of the full board and a committee, or multiple committees. The proxy statement may also be silent regarding CRO responsibility. There are 3 proxy statement sections that this information most often falls: 1) board oversight of risk management, 2) committee-level description or committee-assigned responsibilities, and 3) a paragraph specifically discussing CRO.
   b. Definition: Equal to one if the firm discloses to which governance party CRO is assigned (e.g., to the board, to a committee, or to a combination thereof), and zero otherwise.
   c. Examples from proxy disclosures:
      i. Board (only) Assignment: "*To ensure vigilant monitoring of risks, the Board maintains oversight of our enterprise risk management process and significant risks, including: cybersecurity risks; strategic and operational risks; reputational, brand and legal risks; and environmental and sustainability risks*" (LA-Z-BOY Inc 2021)
      ii. Committee (only) Assignment: "*The audit committee provides oversight concerning our major financial risks and the steps management has taken to monitor and control such exposure, including with respect to the capital, regulatory, and other requirements of our Zillow Offers, Zillow Home Loans, and Zillow Closing Services businesses, and data privacy, cybersecurity, and other topics related to our information technology infrastructure."* (Zillow Group, Inc. 2021)
      iii. Both Board and Committee Assignment: "*Our Board of Directors and the Risk Committee of the Board of Directors oversee an enterprise-wide approach to risk management, including cybersecurity risks, intended to support the achievement of organizational objectives, including strategic objectives, to improve long-term organizational performance and enhance stockholder value*." (Hilltop Holdings Inc. 2021)

2. **Director qualifications relating to cybersecurity**
   a. Background: Firms may disclose that board members have relevant work experience or certifications in areas that enable them to be good monitors of management. Boards may provide this information as part of director biographies, or using a skills matrix, listing director names across the top and desired skillsets down the side, with dots or checkmarks indicating which directors provide which skillset. Firms may also disclose special training and certificate programs that the board, committee, or individual directors complete to bolster their ability to oversee cybersecurity risk. One common example of an external certificate training program includes the CERT Certificate in Cyber-Risk

Oversight Program offered jointly by the National Association of Corporate Directors (NACD) and Carnegie Mellon University.[25]

b. Definition: Equal to one if a keyword relating to technology, cybersecurity, data security, or information security appears in the section of the proxy statement dedicated to director profiles, including qualifications, certifications, or cyber-related training, and zero otherwise.

c. Examples from a proxy disclosure:

   i. "*The Board highly values Mr. McKinley's extensive background in managing complex global technology operations as chief technology officer at a number of leading global companies. This experience is particularly important as we seek to leverage our cloud data and technology transformation to accelerate innovation and new products. These skills are also highly relevant to the Board's oversight of risks and opportunities in our technology operations, including data and cybersecurity, risk management and capital investments. The Board also values his technology and industry experience gained from his twelve years as a partner in Ernst & Young's financial services technology practice, as well as his entrepreneurial insights*." (Equifax Inc 2021)

   ii. Example of a skills matrix (Equifax Inc 2021):

Board Skills Matrix

The Board skills matrix below represents some of the key skills that our Board has identified as particularly valuable to the effective oversight of the Company and the execution of our strategy. This matrix highlights the depth and breadth of the skills of our directors standing for election.

Experience, Expertise or Attribute	Begor	Feidler	Hough	Marcus	McGregor	McKinley	Selander	Smith	Tillman	Wilson
Accounting		•	•	•				•		
Consumer Marketing	•	•		•			•			•
Corporate Governance		•	•	•	•		•		•	
Cybersecurity					•	•			•	
Data & Analytics					•	•				•
Equifax Industry Knowledge	•	•		•		•	•			•
Executive Leadership & Business Operations	•	•	•	•	•	•	•	•	•	•
CEO Experience	•			•	•	•	•	•		
CFO Experience	•			•				•		
International Business	•	•	•		•	•	•	•	•	•
Legal/Regulatory		•		•					•	
Mergers & Acquisitions	•	•	•	•	•	•	•	•	•	
Risk Management	•	•	•	•	•	•	•		•	•
Strategy Development	•	•	•	•	•	•	•	•	•	•
Technology					•	•		•		•

3. **Reporting from management to the board on to cybersecurity matters**

   a. Background: It is management's responsibility to create controls, processes, and reports to monitor, assess, and respond to risks. The board acts on behalf of shareholders to monitor management in its risk-mitigation efforts. For material risks, the SEC requires that firms disclose "how a company perceives the role of its board and the relationship between the board and senior management in managing the material risks facing the company" (SEC 2009). Therefore, firms should disclose how senior management reports

[25] See https://www.nacdonline.org/events/detail.cfm?ItemNumber=37092 for further information about this program.

to the board in matters relating to CRO. In the case of cybersecurity risk, firms often name a management point person or group (e.g., CIO, CISO, Head of Internal Audit) that reports to the board or committee overseeing cybersecurity risk. Firms also disclose how often these meetings occur (e.g., annually, quarterly, at board meetings).

b. Definition: Equal to one if the firm discloses information relating to the reporting line between management and the board, including explicitly naming the title(s) or role name(s) of a management-level point person or department that reports to the board on matters relating to cybersecurity threats, developments, and program activity, or the reporting or meeting frequency, and zero otherwise.

c. Example from a proxy disclosure:

   i. "*Given the importance of information security to our company, the Audit Committee receives regular reports from our chief financial officer, our chief information officer and our vice-president of internal audit regarding our program for managing our information security risks, including data privacy and protection risks faced by the company.*" (Ryman Hospitality Properties Inc 2021)

4. Specific cybersecurity program processes and activities

a. Background: Firms may provide stakeholders information about specific cyber-readiness simulations or "fire drill" type exercises to prepare for a possible data breach or other cybersecurity incident (e.g., denial of service, ransomware attack, etc.). These simulations or "table-top" exercises may include topics such as penetration tests, disaster recovery and business continuity exercises, as well as other mitigation practices.

b. Definition: Equal to one if the firm discloses that they participate in some form of simulation drills related to network or data breaches, and zero otherwise.

c. Example from proxy disclosure: "*We continuously develop and enhance controls, processes and systems to protect our networks, computers, systems, and data from attacks or unauthorized access. We facilitate internal and external third-party assessments, network penetration testing, and regular vulnerability scans of both our internal and external cyber security control."* (Regions Bank 2021)

5. Workforce-level cybersecurity training activities

a. Background: Firms may disclose that they require employees to take part in training programs to increase their awareness of data security threats, such as phishing, spoofing, and social engineering, that give bad actors access to a firm's confidential information. Some firms report that this training is in conjunction with onboarding, whereas others report that workforce training occurs at regular intervals (e.g., annually).

b. Definition: Equal to one if the firm discloses a data security awareness training program for employees, contractors, and/or related parties that interact with the firm's networks and data, and zero otherwise.

c. Example from proxy disclosure: "*Our robust information security training program includes: Information security concepts included in our mandatory onboarding Code*

of Conduct training for all employees, Annual information security awareness training for all office workers with a focus on timely, risk-based topics that align to corporate initiatives, … An annual Cyber Security Awareness Month (CSAM) event consisting of educational opportunities and activities for all employees, including internal and external speakers and presentations." (Kimberly Clark Corp 2021)

6. Involvement of the Internal Audit Function (IAF)

a. Background: Firms may disclose the role that the IAF plays a role in cybersecurity preparedness. Proxy statements describe the IAF role in auditing and assessing the firm's cybersecurity program, as well as providing reports to management and the board in CRO matters.

b. Definition: Equal to one if the firm discloses any IAF involvement relating to CRO, and zero otherwise.

c. Example from proxy disclosure: "*The Audit Committee reviews reports of the Company's internal audit department's periodic audits of our information security, data security, and cybersecurity program.*" (South State Corp 2021)

7. Alignment with an external framework

a. Background: Firms may disclose the use of, and alignment with external frameworks, which provide standards that support firms' information security goals. Common frameworks relating to cyber and information security named in proxy filings include:

i. U.S. National Institute of Standards and Technology (NIST) standards [26]

ii. International Organization for Standardization (ISO) 27001 [27]

iii. International Systems Audit and Control Association (ISACA) – Control Objectives for Information and Related Technologies (COBIT) [28]

b. Definition: Equal to one if the firm discloses alignment with one or more external framework, and zero otherwise.

c. Example from proxy disclosure: "*Our security control protocols map directly to multiple security compliance frameworks, including ISO 27001, Sarbanes-Oxley, DFARS (NIST 800-171), Cybersecurity Maturity Model Certification, and stringent privacy regulations, such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA).*" (Parsons Corp 2021)

8. Use of a third-party to assess or audit the cybersecurity program

a. Background: Firms may disclose that they use outside parties to help oversee CRO, including those parties that review, examine, or audit the firms' data security program. In some cases, but not all, the third-party is the firm's external auditor.

b. Definition: Equal to one if the firm discloses the use of a third-party to assess or audit the data security program, and zero otherwise.

[26] See https://www.nist.gov/cyberframework for further information.
[27] See https://www.iso.org/isoiec-27001-information-security.html for further information.
[28] See https://www.isaca.org/resources/cobit for further information.

c. Example from proxy disclosure: "*The company has an ongoing information security training and compliance program that occurs quarterly and is mandatory for all employees, maintains property and casualty insurance that may cover damages caused as a result of a cyber-security event, and is externally audited based on corporate standards aligned to the NIST Cybersecurity Framework*." (Hess Corp 2021)

9. Collaboration with peers or industry groups

a. Background: Firms may disclose that they meet with peers or industry groups to discuss current issues, hear different viewpoints, and learn how other firms are addressing issues. Working with peers allows "best practices" to emerge with respect to cybersecurity risk mitigation efforts, as well as related disclosure.
b. Definition: Equal to one if the firm discloses working collaboratively with a peer group to address data security threats, and zero otherwise.
c. Example from proxy disclosure*: "Management works closely with key stakeholders, including regulators, government agencies, peer institutions, and industry groups, and develops and invests in talent and innovative technology in order to manage cybersecurity and information security risk."* (Dominion Energy, Inc 2021)

10. Use of cybersecurity insurance

a. Background: Firms may disclose that they purchase insurance to transfer the cyber-related risks that cannot be completely mitigated. Cybersecurity insurance helps to minimize the costs associated with data breaches, including those relating to loss of income due to business interruption, data recovery, legal counsel, ransomware payments, as well as regulatory penalties and fines. Some policies limit coverage to first-party costs, such as those noted above, whereas other policies also cover third-party costs, such as payments to those impacted by the breach and lawsuit settlements.
b. Definition: Equal to one if the firm discloses that its insurance policies include coverage relating to cyber- or data-security incidents, and zero otherwise.
c. Example from proxy disclosure: "*NCR's corporate insurance policies include certain information security risk policies that cover network security, privacy and cyber events*." (NCR Corporation 2021)

11. Executive cybersecurity expertise

a. Background: Firms may disclose in the executive biography section of the proxy statement that an executive has cyber- or data-security related expertise.
b. Definition: Equal to one if the firm discloses that at least one executive has cyber- or data-security- related work experience, zero otherwise.
c. Example from proxy disclosure: "*Adam Bonanno, 43, Chief Technology Officer of the Corporation and the Bank, Senior Vice President of the Bank. Mr. Bonanno joined Bryn Mawr Trust in January 2019, bringing 19 years of experience across various aspects of IT management including software development, systems integration,*

cybersecurity, governance, data sciences, and predictive analytics." (Bryn Mawr Bank Corp 2021)

12. Executive compensation discussion includes statements relating to cybersecurity performance or achievements, including Key Performance Indicators (KPIs)

a. Background: Firms may disclose that they link executive compensation to cybersecurity performance. As part of their fiduciary duties, directors are tasked with designing compensation packages that align executives' incentives with long-term company strategies and goals. By including cybersecurity performance, executives can be held more accountable for poor cybersecurity performance, as compared to those who do not have such metrics. As noted in the example below, some firms disclose that the compensation metric can decrease, but not increase, executive compensation.

b. Definition: Equal to one if the firm discloses that cybersecurity-related metrics are a component of executive incentive plans, and zero otherwise.

c. Example from proxy disclosure: "*For the 2020 Annual Incentive Plan, the Committee retained a cybersecurity performance measure as one of the metrics to evaluate performance of all employees, including our NEOs. Achievement of the cybersecurity metric cannot increase the executive's compensation, but failure to meet it will decrease the award*." (Equifax 2021)

Appendix C: Figures

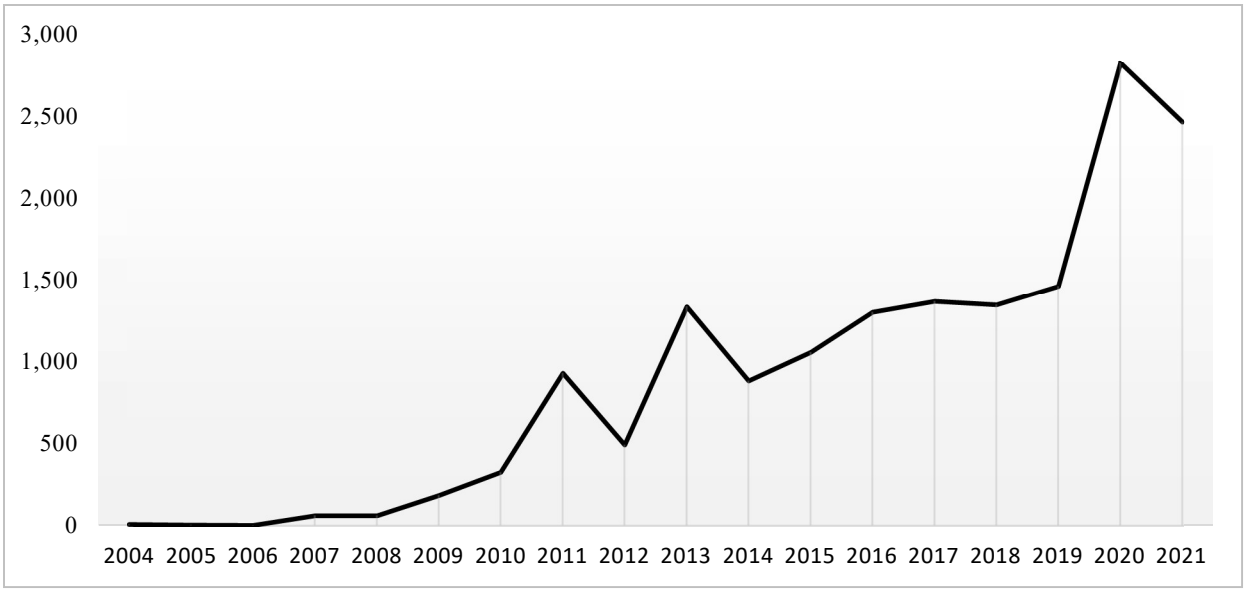

Figure 1: Media Attention on Cybersecurity Incidents

Notes: Figure 1 plots the number of articles published in the Dow Jones Newswires, regional additions of the Wall Street Journal, Barron's and MarketWatch, relating to *firm-specific* data breach incidents from January 1, 2004 through December 31, 2021 (Source: RavenPack News Analytics Dataset).

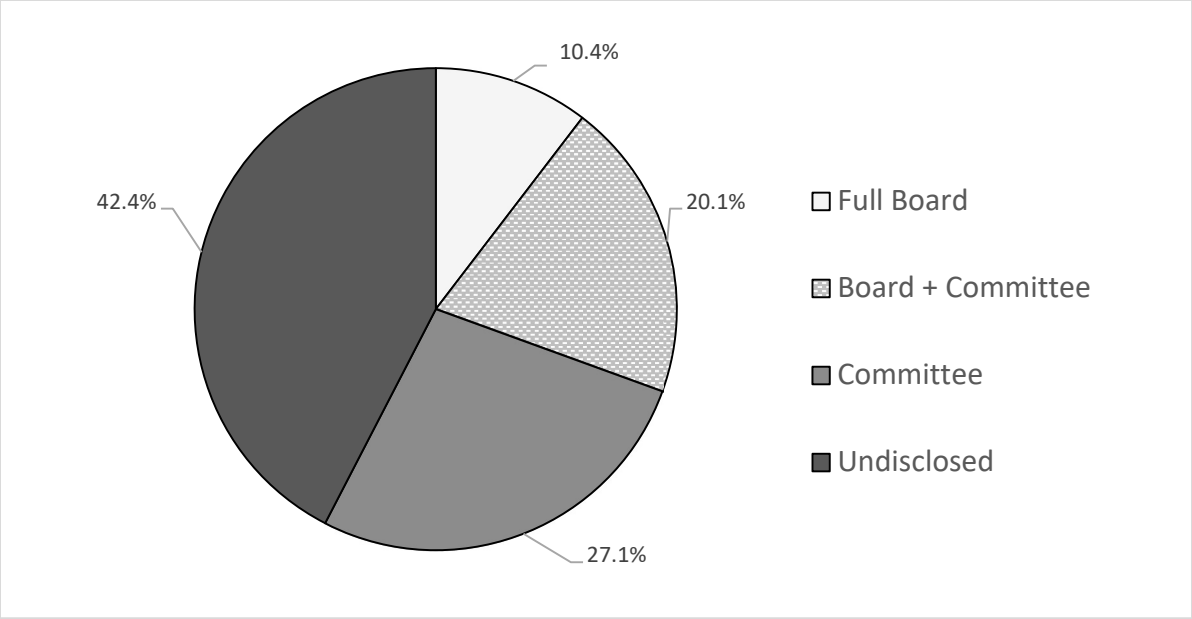

Figure 2: Cybersecurity Risk Oversight Assignment

Notes: Figure 2 presents, using hand-collected data from the full sample (N = 2,921), the proportion of firms that disclose to which board party cybersecurity risk oversight is assigned (57.6%), and whether it is assigned to the full board, to a committee, or to a combination thereof.

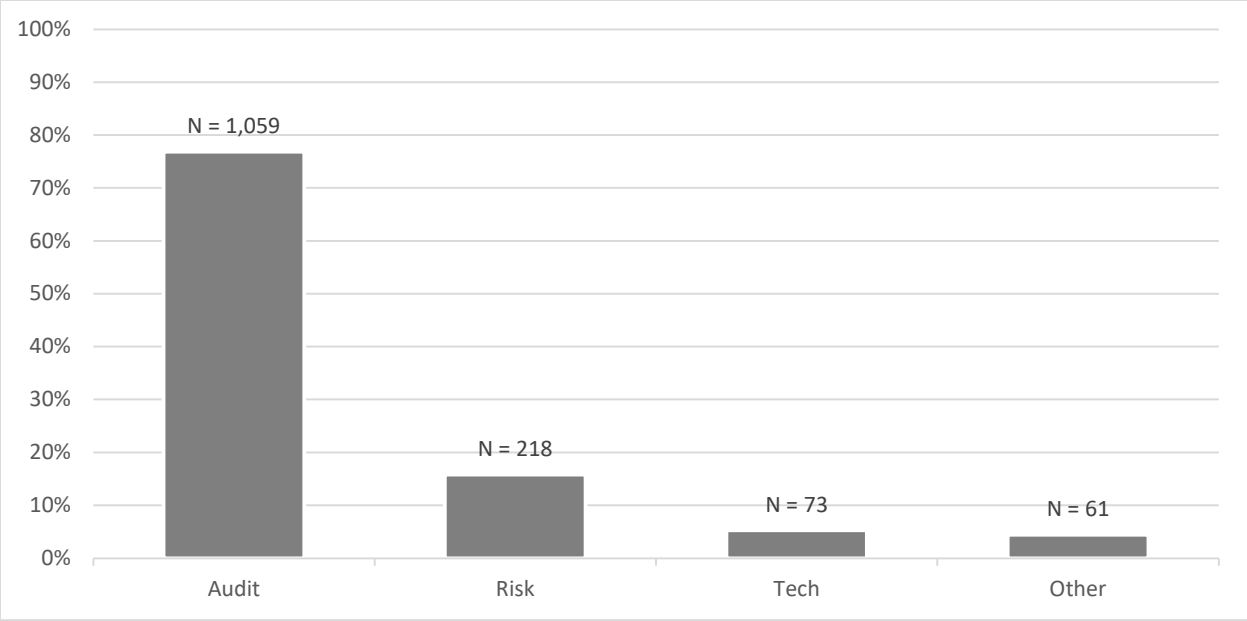

Figure 3: Committee Assignments

Notes: Figure 3 presents, using hand-collected data from the reduced sample of firms that disclose a committee assignment for cybersecurity risk oversight (N = 1,378), the frequency of firms that assign oversight responsibility to the audit committee, the risk committee, the technology committee, or another committee. Note: because a few firms assign CRO to multiple committees, the total of committee assignments can exceed 1,378.

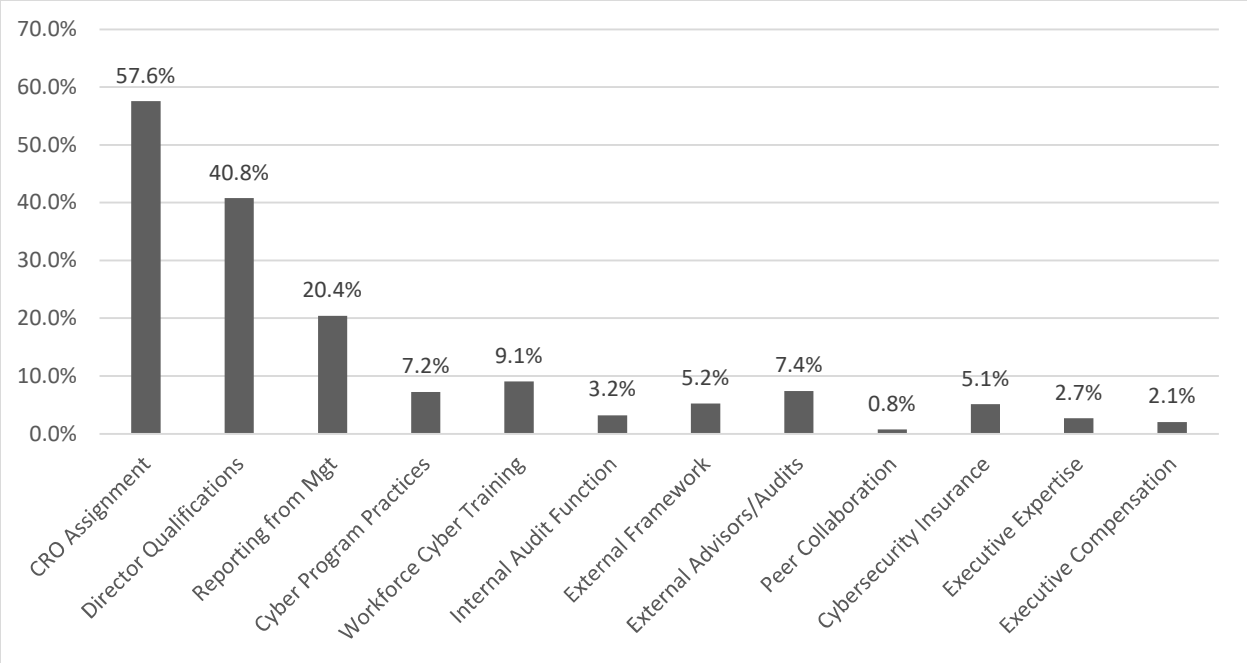

Figure 4: Cybersecurity Risk Oversight Transparency Score (T-Score) Elements

Note: Figure 4 presents, using hand-collected data, the frequency of firms that disclose each of the 12 CRO elements in the full sample (N = 2,921). See Appendix B for further descriptions of each *T-Score* element.

Appendix D: Tables

Table 1: Sample Selection and Composition

Panel A. Sample Selection

Description	Number of Observations
Unique DEF 14A Proxy Statements filed between 1/1/21 and 12/31/21	5,386
Less: Observations that do not merge with required datasets	(1,421)
Less: Firms that that do not include a cyber-related risk in Item 1A in the most recent 10-K Annual Report	(315)
Less: Observations with missing variables to construct models	(729)
Proxy Statement – Total Sample	**2,921**

Panel B. Observations by Industry (Fama-French 12)

	Industry	N	%	Mean *T-Score*
(1)	Consumer Nondurables	114	0.04	1.60
(2)	Consumer Durables	63	0.02	1.35
(3)	Manufacturing	242	0.08	1.66
(4)	Oil, Gas and Coal Extraction and Products	83	0.03	1.08
(5)	Chemicals and Allied Products	66	0.02	1.68
(6)	Business Equipment	440	0.15	2.06
(7)	Telephone and Television Transmission	38	0.01	1.71
(8)	Utilities	63	0.02	2.54
(9)	Wholesale, Retail and Some Services	215	0.07	1.86
(10)	Healthcare, Medical Equipment and Drugs	545	0.19	0.90
(11)	Financial Institutions	748	0.26	1.70
(12)	Other	304	0.10	1.82
	Total	**2,921**	**1.00**	**1.62**

Notes: This table presents the sample selection and distribution. Panel A reports the sample construction, beginning with all Proxy Statements filed in 2021. I remove observations that do not merge with required datasets, those firms that do not report a material cyber-related risk in the 10-K filing in closest proximity to the 2021 proxy statement, those missing required variables, and those later to be found during the hand-collection validation process relating to a special meeting. Panel B reports the distribution of observations across industries, following the Fama-French 12 industry classification, as well as the average industry *T-Score*, which represents the number of cybersecurity program elements disclosed by a firm in the sample.

Table 2: Descriptive Statistics

Panel A: Descriptive Statistics for the Sample Used in the Estimation of Model (1)

Variable	N	Mean	Std. Dev.	Min.	25%	Median	75%	Max.
Discl_Assign	2,921	0.58	0.49	0.00	0.00	1.00	1.00	1.00
Discl_Qual	2,921	0.41	0.49	0.00	0.00	0.00	1.00	1.00
Discl_Report	2,921	0.20	0.40	0.00	0.00	0.00	0.00	1.00
Discl_Process	2,921	0.22	0.41	0.00	0.00	0.00	0.00	1.00
T_Score	2,921	1.62	1.76	0.00	0.00	1.00	2.00	10.00
High_IndBreach	2,921	0.50	0.50	0.00	0.00	0.00	1.00	1.00
FirmSize	2,921	7.24	2.06	2.94	5.74	7.26	8.62	12.24
InstInvest	2,921	0.60	0.34	0.00	0.33	0.72	0.89	1.00
BoardSize	2,921	8.75	2.36	4.00	7.00	9.00	10.00	15.00
MultiBd_Dir	2,921	0.44	0.23	0.00	0.29	0.43	0.60	1.00
IT_Expert	2,921	0.21	0.41	0.00	0.00	0.00	0.00	1.00
Big4	2,921	0.69	0.46	0.00	0.00	1.00	1.00	1.00
FirmAge	2,921	2.85	0.85	1.10	2.08	3.04	3.50	4.25
ROA	2,921	-0.09	0.33	-1.90	-0.08	0.01	0.05	0.33
Growth	2,921	5.29	9.16	0.37	1.20	2.37	5.03	65.82
Leverage	2,921	0.27	0.21	0.00	0.07	0.25	0.42	0.82
Loss	2,921	0.41	0.49	0.00	0.00	0.00	1.00	1.00
Returns	2,921	0.07	0.69	-0.77	-0.29	-0.11	0.18	3.70
MWeak	2,921	0.04	0.19	0.00	0.00	0.00	0.00	1.00
Lit_Indus	2,921	0.32	0.47	0.00	0.00	0.00	1.00	1.00
Merger	2,921	0.33	0.47	0.00	0.00	0.00	1.00	1.00
Foreign	2,921	0.50	0.50	0.00	0.00	0.00	1.00	1.00
NYSE	2,921	0.41	0.49	0.00	0.00	0.00	1.00	1.00
Length	2,921	10.27	0.49	9.12	9.95	10.25	10.57	11.58

Notes: This table reports descriptive statistics for the variables used in my tests. I winsorize all continuous variables at the 1st and 99th percentiles. All variables are defined in Appendix A.

Table 2 Continued

Panel B: Univariate Test of Means Between Non-Disclosers and Disclosers

Variable	*Cyber_Disclosure* = 0		*Cyber_Disclosure* = 1		Difference	
High_IndBreach	0.410	[0.00]	0.550	[0.00]	0.145***	[0.000]
FirmSize	5.970	[0.00]	7.960	[0.00]	1.988***	[0.000]
InstInvest	0.460	[0.00]	0.680	[0.00]	0.217***	[0.000]
BoardSize	7.520	[0.00]	9.440	[0.00]	1.922***	[0.000]
MultiBd_Dir	0.390	[0.00]	0.470	[0.00]	0.081***	[0.000]
IT_Expert	0.100	[0.00]	0.270	[0.00]	0.169***	[0.000]
Big4	0.470	[0.00]	0.810	[0.00]	0.338***	[0.000]
FirmAge	2.570	[0.00]	3.010	[0.00]	0.447***	[0.000]
ROA	-0.210	[0.00]	-0.020	[0.00]	0.195***	[0.000]
Growth	4.640	[0.00]	5.650	[0.00]	1.011***	[0.004]
Leverage	0.230	[0.00]	0.290	[0.00]	0.058***	[0.000]
Loss	0.550	[0.00]	0.330	[0.00]	-0.216***	[0.000]
Returns	0.120	[0.00]	0.040	[0.00]	-0.083***	[0.002]
MWeak	0.050	[0.00]	0.030	[0.00]	-0.012*	[0.099]
Lit_Indus	0.370	[0.00]	0.290	[0.00]	-0.085***	[0.000]
Merger	0.240	[0.00]	0.380	[0.00]	0.148***	[0.000]
Foreign	0.350	[0.00]	0.580	[0.00]	0.236***	[0.000]
NYSE	0.230	[0.00]	0.520	[0.00]	0.291***	[0.000]
Length	10.030	[0.00]	10.410	[0.00]	0.387***	[0.000]
N	1,053		1,868		2,921	

Notes: This table reports the results of a univariate test of means between firms that are silent with regard to cybersecurity oversight (*Cyber_Disclosure* = 0), as compared to those that disclose *at least one* cybersecurity oversight program element (*Cyber_Disclosure* = 1). I winsorize all continuous variables at the 1st and 99th percentiles. p-values are based on two-sample t-test for the test of difference in means. *, **, and *** denote statistical significance at the 10, 5, and 1 percent levels, respectively.

Table 2 Continued

Panel C: Pairwise Correlations

	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)	(13)	(14)	(15)	(16)	(17)	(18)	(19)	(20)	(21)	(22)	(23)	(24)
(1) *Discl_Assign*	1.00																							
(2) *Discl_Qual*	**0.50**	1.00																						
(3) *Discl_Report*	**0.41**	**0.25**	1.00																					
(4) *Discl_Process*	**0.35**	**0.30**	**0.46**	1.00																				
(5) *T_Score*	**0.69**	**0.62**	**0.68**	**0.75**	1.00																			
(6) *High_IndBreach*	**0.15**	**0.09**	**0.11**	**0.09**	**0.14**	1.00																		
(7) *FirmSize*	**0.46**	**0.31**	**0.29**	**0.25**	**0.41**	**0.16**	1.00																	
(8) *InstInvest*	**0.31**	**0.23**	**0.16**	**0.15**	**0.25**	**0.12**	**0.45**	1.00																
(9) *BoardSize*	**0.36**	**0.26**	**0.27**	**0.21**	**0.34**	0.00	**0.54**	**0.30**	1.00															
(10) *MultiBd_Dir*	**0.19**	**0.14**	**0.11**	**0.11**	**0.18**	**-0.08**	**0.32**	**0.17**	**0.21**	1.00														
(11) *IT_Expert*	**0.18**	**0.22**	**0.11**	**0.12**	**0.20**	**0.13**	**0.19**	**0.16**	**0.17**	0.01	1.00													
(12) *Big4*	**0.36**	**0.22**	**0.19**	**0.17**	**0.28**	**0.12**	**0.57**	**0.36**	**0.30**	**0.31**	**0.13**	1.00												
(13) *FirmAge*	**0.23**	**0.11**	**0.20**	**0.11**	**0.20**	**0.21**	**0.28**	**0.19**	**0.28**	**-0.09**	**0.07**	**0.10**	1.00											
(14) *ROA*	**0.26**	**0.15**	**0.17**	**0.14**	**0.23**	**0.24**	**0.36**	**0.25**	**0.27**	**-0.05**	**0.07**	**0.18**	**0.38**	1.00										
(15) *Growth*	**0.07**	**0.09**	**0.04**	**0.05**	**0.09**	**0.06**	**0.27**	**0.12**	0.01	**0.11**	**0.11**	**0.11**	**-0.08**	**-0.08**	1.00									
(16) *Leverage*	**0.16**	**0.07**	**0.10**	**0.08**	**0.14**	**0.19**	**0.18**	-0.02	**0.05**	**0.10**	0.01	**0.27**	**0.08**	**0.15**	**0.18**	1.00								
(17) *Loss*	**-0.19**	**-0.11**	**-0.15**	**-0.11**	**-0.19**	**-0.09**	**-0.33**	**-0.12**	**-0.29**	**0.07**	**-0.06**	**-0.05**	**-0.35**	**-0.56**	**0.06**	**0.05**	1.00							
(18) *Returns*	**-0.06**	-0.01	**-0.06**	**-0.05**	**-0.06**	**0.08**	**0.11**	**0.06**	**-0.14**	-0.01	**0.04**	-0.02	**-0.15**	**-0.09**	**0.25**	**-0.07**	**0.05**	1.00						
(19) *MWeak*	**-0.03**	-0.01	-0.02	-0.03	**-0.04**	0.02	**-0.06**	0.02	**-0.05**	**-0.05**	-0.01	**-0.07**	-0.03	-0.03	-0.01	-0.01	**0.06**	0.01	1.00					
(20) *Lit_Indus*	**-0.07**	**0.04**	**-0.08**	**-0.04**	**-0.05**	**-0.05**	**-0.03**	**0.08**	**-0.19**	**0.13**	**0.08**	**0.03**	**-0.28**	**-0.30**	**0.23**	**-0.10**	**0.29**	**0.22**	0.02	1.00				
(21) *Merger*	**0.14**	**0.13**	**0.09**	**0.07**	**0.14**	**0.10**	**0.23**	**0.26**	**0.16**	**0.07**	**0.09**	**0.12**	**0.09**	**0.14**	0.02	**0.07**	**-0.09**	0.01	0.02	-0.02	1.00			
(22) *Foreign*	**0.23**	**0.16**	**0.10**	**0.09**	**0.17**	**0.18**	**0.30**	**0.35**	**0.07**	**0.11**	**0.15**	**0.26**	**0.10**	**0.08**	**0.19**	**0.08**	**0.05**	**0.10**	**0.04**	**0.16**	**0.25**	**1.00**		
(23) *NYSE*	**0.28**	**0.13**	**0.19**	**0.15**	**0.24**	**0.12**	**0.40**	**0.13**	**0.27**	**0.11**	**0.06**	**0.36**	**0.24**	**0.25**	-0.02	**0.33**	**-0.16**	**-0.11**	-0.03	**-0.29**	**0.07**	**0.12**	**1.00**	
(24) *Length*	**0.38**	**0.26**	**0.27**	**0.23**	**0.36**	**0.09**	**0.50**	**0.30**	**0.39**	**0.23**	**0.16**	**0.37**	**0.26**	**0.15**	**0.09**	**0.20**	**-0.08**	**-0.04**	0.00	-0.03	**0.16**	**0.25**	**0.31**	**1.00**

Notes: This table reports pairwise correlations for the variables used in my tests with all variables (N = 2,921). I winsorize all continuous variables at the 1st and 99th percentiles. Correlations in **bold** are statistically different from zero at the 10 percent level. All variables are defined in Appendix A.

Table 3: The Determinants of Cybersecurity Risk Oversight (CRO) Disclosures

		(1)		(2)	
		DV = *Discl_Assign*		**DV = *Discl_Qual***	
Variables	**Predicted Sign**	**Coeff.**	**p-val**	**Coeff.**	**p-val**
Constant		-12.093***	0.000	-7.791***	0.000
LEVEL OF CYBER RISK					
High_IndBreach	*?*	0.255***	0.009	0.119	0.181
STAKEHOLDER DEMAND					
FirmSize	+	0.243***	0.000	0.092***	0.006
InstInvest	+	0.367***	0.009	0.464***	0.001
BOARD RESOURCES					
BoardSize	+	0.124***	0.000	0.105***	0.000
MultiBd_Dir	+	0.661***	0.002	0.412**	0.021
IT_Expert	+	0.530***	0.000	0.718***	0.000
Big4	+	0.299***	0.006	0.147	0.108
CONTROL VARIABLES					
FirmAge		0.115*	0.068	-0.061	0.288
ROA		0.576***	0.007	0.462**	0.018
Growth		-0.006	0.283	0.003	0.548
Leverage		0.395*	0.095	0.098	0.664
Loss		-0.152	0.205	-0.130	0.237
Returns		-0.253***	0.001	-0.104	0.147
MWeak		-0.062	0.786	0.066	0.756
Lit_Indus		0.034	0.765	0.361***	0.001
Merger		-0.124	0.230	0.141	0.122
Foreign		0.408***	0.000	0.100	0.292
NYSE		0.166	0.127	0.024	0.813
Length		0.799***	0.000	0.487***	0.000
Observations		2,921		2,921	
Area under ROC curve		0.823		0.733	

Table 3 Continued

Variables	Predicted Sign	(3) DV = *Discl_Report* Coeff.	p-val	(4) DV = *Discl_Process* Coeff.	p-val
Constant		-11.440***	0.000	-9.050***	0.000
LEVEL OF CYBER RISK					
High_IndBreach	*?*	0.224**	0.039	0.241**	0.019
STAKEHOLDER DEMAND					
FirmSize	+	0.065*	0.062	0.081**	0.023
InstInvest	+	0.288*	0.060	0.291**	0.048
BOARD RESOURCES					
BoardSize	+	0.137***	0.000	0.079***	0.002
MultiBd_Dir	+	0.415*	0.060	0.464**	0.030
IT_Expert	+	0.180*	0.065	0.322***	0.003
Big4	+	0.258*	0.053	0.121	0.206
CONTROL VARIABLES					
FirmAge		0.128*	0.073	-0.129*	0.058
ROA		1.924***	0.002	0.966***	0.003
Growth		0.001	0.882	0.003	0.542
Leverage		0.356	0.190	0.053	0.841
Loss		0.041	0.798	-0.061	0.648
Returns		-0.294**	0.018	-0.250**	0.017
MWeak		-0.005	0.986	-0.232	0.390
Lit_Indus		-0.023	0.861	-0.024	0.841
Merger		0.014	0.893	-0.001	0.994
Foreign		0.036	0.750	0.020	0.851
NYSE		0.196*	0.095	0.186	0.102
Length		0.675***	0.000	0.588***	0.000
Observations		2,921		2,921	
Area under ROC curve		0.771		0.772	

Notes: This table reports the results from estimating Model (1), which uses logistic regression to test the relation between firm characteristics and three different oversight disclosure outcomes. In Column (1), the dependent variable, *Discl_Assign* is an indicator variable equal to one if the firm discloses how the responsibility for cybersecurity risk oversight is allocated across the board, and zero otherwise. In Column (2), the dependent variable*, Discl_Qual*, is an indicator variable equal to one if the firm discloses that a board member has work experience or certifications relating to technology or cybersecurity, and zero otherwise. In Column (4), the dependent variable, *Discl_Report* is an indicator variable equal to one if the firm how senior management reports to the board on CRO matters, and zero otherwise. Finally, in Column (3), the dependent variable, *Discl_Process,* is an indicator equal to one if the firm discloses at least one other oversight element (i.e., not relating to oversight assignment, nor director qualification), and zero otherwise. I winsorize all continuous variables at the 1st and 99th percentiles. *, **, and *** denote statistical significance at the 10, 5, and 1 percent levels, respectively, based on two-tailed tests (one-tailed when there is a predicted sign). All variables are defined in Appendix A.

Table 4: The Transparency Score (*T-Score*) Model

Variables	Predicted Sign	(1) DV = *T-Score* Coeff.	p-val	(3) DV = *T-Score* Coeff.	p-val	DV = *T-Score* Coeff.	p-val
Intercept		-6.345***	0.000	-2.990***	0.000	-2.094**	0.033
CRO_BoardOnly	?			1.984***	0.000		
CRO_CommOnly	?			1.959***	0.000		
CRO_Shared	?			2.598***	0.000		
CRO_AuditComm	?					0.076	0.407
CRO_RiskComm	?					0.300**	0.044
CRO_TechComm	?					0.168	0.403
CRO_OtherComm	?					0.037	0.853
LEVEL OF CYBER RISK							
High_IndBreach	?	0.197***	0.001	0.091*	0.067	0.141*	0.081
STAKEHOLDER DEMAND							
FirmSize	+	0.105***	0.000	0.011	0.286	0.007	0.417
InstInvest	+	0.201**	0.032	-0.020	0.409	0.075	0.295
BOARD RESOURCES							
BoardSize	+	0.087***	0.000	0.037***	0.002	0.039*	0.051
MultiBd_Dir	+	0.486***	0.001	0.275***	0.006	0.444**	0.013
IT_Expert	+	0.430***	0.000	0.236***	0.000	0.236**	0.006
Big4	+	0.055	0.246	-0.114**	0.028	-0.181*	0.073
CONTROL VARIABLES							
FirmAge		0.038	0.296	0.001	0.975	-0.053	0.322
ROA		0.222***	0.010	0.026	0.666	0.048	0.836
Growth		0.004	0.306	0.006	0.109	0.009*	0.089
Leverage		0.245	0.117	0.052	0.669	0.222	0.299
Loss		-0.213***	0.004	-0.146**	0.011	-0.214**	0.034
Returns		-0.147***	0.000	-0.065**	0.018	-0.141**	0.047
MWeak		-0.104	0.394	-0.075	0.370	-0.066	0.672
Lit_Indus		0.078	0.269	0.088	0.114	0.156	0.116
Merger		0.046	0.490	0.090	0.101	0.109	0.207
Foreign		0.095	0.136	-0.062	0.228	-0.118	0.182
NYSE		0.158**	0.030	0.071	0.223	0.084	0.342
Length		0.550***	0.000	0.270***	0.000	0.387***	0.000
Observations		2,921		2,921		1,682	
Adjusted R^2		0.243		0.519		0.048	

Table 4 Continued

Notes: This table reports the results from estimating Model (1) using ordinary least squares regression to examine the relation between firm characteristics and the level of risk oversight disclosure, the Transparency Score (*T-Score*). Column (1) examines the influence of firm characteristics on disclosure in the full sample. Column (2) examines the influence of the various parties assigned CRO responsibility, relative to firms that do not disclose CRO assignment. *CRO_BoardOnly* is an indicator equal to one for firms that disclose that the board, and the board alone, retains oversight responsibility, and zero otherwise. *CRO_CommOnly* is an indicator equal to one for firms that disclose that the board has delegated CRO to a committee, and zero otherwise. *CRO_Shared* is an indicator equal to one for firms that disclose that the board and a specified committee share CRO responsibility, and zero otherwise. Column (3) limits the sample to those firms disclosing which party is assigned CRO responsibility, and examines the impact of committee assignments, relative to those firms with CRO responsibility retained by the full board. Each committee type is a separate indicator variable: *CRO_AuditComm*, *CRO_RiskComm*, *CRO_TechComm*, *CRO_OtherComm*. I winsorize all continuous variables at the 1st and 99th percentiles. *, **, and *** denote statistical significance at the 10, 5, and 1 percent levels, respectively, based on two-tailed tests (one-tailed when there is a predicted sign). All independent variables are defined in Appendix A. *T-Score* elements are further described in Appendix B.

Table 5: The Transparency Score (*T-Score*) Model – Cross-Sectional Analyses

	Risk Committee vs. non-Risk Committee Firms			
	(1)		(2)	
	DV = *T-Score*		**DV = *T-Score***	
Variables	**Coeff.**	**p-val**	**Coeff.**	**p-val**
Constant	-8.137***	0.004	-5.982***	0.000
LEVEL OF CYBER RISK				
High_IndBreach	0.196	0.351	0.229***	0.000
STAKEHOLDER DEMAND				
FirmSize	-0.072	0.213	0.122***	0.000
InstInvest	1.089***	0.004	0.081	0.233
BOARD RESOURCES				
BoardSize	0.103**	0.028	0.074***	0.000
MultiBd_Dir	0.466	0.216	0.459***	0.001
IT_Expert	0.576***	0.009	0.378***	0.000
Big4	0.223	0.230	0.050	0.268
CONTROL VARIABLES				
FirmAge	0.119	0.416	0.033	0.368
ROA	-0.653	0.737	0.230***	0.009
Growth	-0.020*	0.095	0.007	0.105
Leverage	1.141**	0.041	0.175	0.269
Loss	-0.239	0.410	-0.186**	0.014
Returns	0.260	0.447	-0.161***	0.000
MWeak	-0.245	0.618	-0.115	0.361
Lit_Indus	0.447	0.264	0.084	0.232
Merger	0.015	0.947	0.050	0.462
Foreign	-0.136	0.606	0.162**	0.011
NYSE	0.255	0.296	0.148**	0.048
Length	0.770**	0.015	0.514***	0.000
Observations	368		2,553	
Sample Firms	Firms w/ Risk Committees		Firms w/o Risk Committees	
Adjusted R^2	0.143		0.248	

Table 5 Continued

	Breached vs. non-Breached Firms			
	(3)		(4)	
	DV = *T-Score*		**DV = *T-Score***	
Variables	**Coeff.**	**p-val**	**Coeff.**	**p-val**
Constant	2.183	0.415	-7.011***	0.000
LEVEL OF CYBER RISK				
High_IndBreach	0.685**	0.014	0.174***	0.006
STAKEHOLDER DEMAND				
FirmSize	0.139*	0.065	0.108***	0.000
InstInvest	-0.065	0.440	0.208**	0.033
BOARD RESOURCES				
BoardSize	0.077	0.104	0.084***	0.000
MultiBd_Dir	1.230**	0.024	0.434***	0.002
IT_Expert	0.344*	0.066	0.446***	0.000
Big4	0.277	0.259	0.036	0.329
CONTROL VARIABLES				
FirmAge	0.012	0.934	0.039	0.302
ROA	-0.647	0.267	0.231***	0.008
Growth	0.024	0.172	0.003	0.523
Leverage	-0.363	0.533	0.273*	0.095
Loss	-0.197	0.538	-0.229***	0.003
Returns	-0.429**	0.023	-0.137***	0.001
MWeak	-1.209***	0.005	-0.075	0.558
Lit_Indus	-0.299	0.178	0.121	0.106
Merger	0.217	0.362	0.040	0.567
Foreign	-0.114	0.647	0.114*	0.089
NYSE	0.269	0.251	0.137*	0.070
Length	-0.323	0.282	0.618***	0.000
Observations	236		2,685	
Sample Firms	Breached Firms		Non-Breached Firms	
Adjusted R^2	0.177		0.243	

Notes: This table reports cross-sectional results examining the relation between firm characteristics and the overall level of risk oversight disclosure. Using an ordinary least squares model, I regress the Transparency Score (*T-Score*), on the firm characteristics in Model (1) using the full sample. Columns (1) and (2) present the results for firms with risk committees (1) and without risk committees (2). Columns (3) and (4) present the results for firms that have reported a data breach (3) and those firms that have not reported a breach (4) in the prior 3 years. I winsorize all continuous variables at the 1st and 99th percentiles. *, **, and *** denote statistical significance at the 10, 5, and 1 percent levels, respectively, based on two-tailed tests (one-tailed when there is a predicted sign). All independent variables are defined in Appendix A. *T-Score* elements are further described in Appendix B.

Table 6: The Frequency of *T-Score* Elements by Industry

		Industry Classification (Fama-French 12)											
		1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**
T-Score Elements	***N=*** **2,921**	114	63	242	83	66	440	38	63	215	545	748	304
1) ***CRO Assignment***	0.58	0.63	0.60	0.66	0.51	0.62	0.67	0.58	0.86	0.67	0.36	0.57	0.65
2) ***Director Qualifications***	0.41	0.28	0.37	0.40	0.28	0.38	0.60	0.42	0.62	0.42	0.28	0.39	0.44
3) ***Reporting from Mgt***	0.20	0.24	0.17	0.22	0.11	0.20	0.24	0.24	0.37	0.27	0.08	0.23	0.25
4) ***Cyber Program Practices***	0.07	0.07	0.05	0.05	0.01	0.09	0.10	0.13	0.13	0.08	0.03	0.09	0.06
5) ***Workforce Cyber Training***	0.09	0.08	0.05	0.11	0.01	0.15	0.08	0.11	0.19	0.11	0.04	0.12	0.10
6) ***Internal Audit Function***	0.03	0.08	0.00	0.01	0.02	0.03	0.03	0.05	0.02	0.04	0.01	0.03	0.06
7) ***External Framework***	0.05	0.03	0.05	0.06	0.02	0.09	0.08	0.05	0.06	0.07	0.02	0.05	0.07
8) ***External Advisors/Audits***	0.07	0.11	0.03	0.06	0.06	0.03	0.09	0.03	0.14	0.10	0.04	0.08	0.08
9) ***Peer Collaboration***	0.01	0.02	0.00	0.00	0.00	0.02	0.01	0.00	0.05	0.00	0.00	0.01	0.00
10) ***Cybersecurity Insurance***	0.05	0.05	0.00	0.05	0.05	0.05	0.05	0.05	0.05	0.09	0.02	0.07	0.05
11) ***Executive Expertise***	0.03	0.01	0.03	0.01	0.00	0.00	0.08	0.00	0.05	0.01	0.01	0.03	0.03
12) ***Executive Compensation***	0.02	0.00	0.00	0.02	0.01	0.03	0.02	0.05	0.02	0.00	0.01	0.03	0.03
Total T-Score	**1.62**	**1.60**	**1.35**	**1.66**	**1.08**	**1.68**	**2.06**	**1.71**	**2.54**	**1.86**	**0.90**	**1.70**	**1.82**

Notes: This table reports the frequency of each *T-Score* element for each industry classification in my full sample (N = 2,921). The Fama-French 12 industries are classified as: 1) consumer nondurables, 2) consumer durables, 3) manufacturing, 4) oil, gas, and coal extraction and products, 5) chemicals and allied products, 6) business equipment, 7) telephone and television transmission, 8) utilities, 9) wholesale, retail, and some services, 10) healthcare, medical equipment, and drugs, 11) financial institutions, and 12) other. The greyscale coloring is conditionally formatted such that, for each *T-Score* element, the darker (lighter) the shading, the higher (lower) the disclosure frequency across all 12 industry sectors. All *T-score* elements are defined in Appendix B.

Vita

Laurie Ereddia is from Atlanta, Georgia. She earned her Bachelor of Business Administration in Accounting and her Master of Accounting degrees at Kennesaw State University. Before joining the doctoral program, she worked as an audit associate at Grant Thornton in Atlanta, Georgia, and as a controller at a small private entity. Laurie also worked as an adjunct instructor of introductory financial accounting at Kennesaw State. She is a licensed CPA in the state of Georgia. At the University of Tennessee, Laurie was the lead instructor for an undergraduate auditing class. Her research interests are in auditing, financial reporting, and corporate governance. Laurie will begin her academic career as a tenure-track assistant professor at Mississippi State University in the fall of 2023.