# Three Essays on the Governance of Cybersecurity

Farzaneh Amani

A Thesis

In

The John Molson School of Business

Presented in Partial Fulfillment of the Requirements

For the Degree of

Doctor of Philosophy (Business Administration) at

Concordia University

Montreal, Quebec, Canada

June 2023

**CONCORDIA UNIVERSITY**

**SCHOOL OF GRADUATE STUDIES**

This is to certify that the thesis prepared

By: Farzaneh Amani

Entitled: Three Essays on the Governance of Cybersecurity

and submitted in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY (*Accountancy*)

complies with the regulations of the University and meets the accepted standards with respect to originality and quality.

Signed by the final examining committee:

Chair

Dr. Michele Paulin

External Examiner

Dr. Lyne Bouchard

External to Program

Dr. Dongyoung Lee

Examiner

Dr. Elisabeth Peltier

Thesis Co-Supervisor

Dr. Michel Magnan

Thesis Co-Supervisor

Dr. Rucsandra Moldovan

Approved by

Dr. Cédric Lesage, Graduate Program Director

June 19, 2023

Dr. Anne-Marie Croteau, Dean
John Molson School of Business

**Abstract**

**Three Essays on the Governance of Cybersecurity**

**Farzaneh Amani, Ph.D.**

**Concordia University, 2023**

This dissertation consists of three interrelated essays that examine the governance of cybersecurity. The first essay synthesizes the literature on the of cybersecurity risks and incidents to identify its drivers, informativeness, quality, theoretical perspectives, and future directions. The review identifies several drivers for cybersecurity disclosure, highlights that while the level of informativeness of such disclosure meets the usefulness expectations of regulators, its quality falls short, mostly lacks an explicit theoretical framework, and uses predominantly textual content analysis and event studies. The review identifies the need for research in both governance and management of cybersecurity disclosure, thus providing the motivation for the second and third essays. The second essay examines where cybersecurity risk oversight resides within a firm's governance structure, what determines such positioning, and how it impacts the firm's response to a cybersecurity breach. In proxy statements, breached firms explicitly disclose oversight assignment with a wide variation, ranging from full board to a named board committee - the audit committee being the most common. Results show that board connectedness and cyber competency are positively associated with oversight assignment, full board oversight is more likely with smaller boards, and boards' shareholding and cyber competency steer oversight to the audit committee. In the event of a breach, the presence of oversight decreases the time firms take to announce and resolve the breach, as well as reduces the recurrence of breaches. While the audit committee cybersecurity oversight discloses and resolves the breach quicker, full board oversight

leads to fewer recurrences. The increase of data breaches leads firms to adopt various risk management strategies, hence the third essay examines the relation between cyber insurance disclosure and a firm's likelihood of being target of a future breach. Using textual analysis of the risk factors disclosed in 10-K filings and comparing cyber insurance disclosures of firms that are breached to those that are not, the evidence shows that firms disclosing cyber insurance have a significantly higher subsequent probability of being breached. Furthermore, it appears that disclosing cyber insurance leads to delayed public breach disclosure but more timely breach resolution, and higher breach recurrence.

Keywords: Cybersecurity; Literature Review; Disclosure; Cybersecurity Risks and Incidents; Risk Oversight; Corporate Governance; Data Breaches; Determinants; Consequences; Cyber Insurance; Risk Management; Risk Transfer

**Acknowledgements**

First and foremost, I thank God (Allah) for blessing me with health, strength, and perseverance to complete this dissertation. I would like to express my deepest appreciation to both my co-supervisors Prof. Michel Magnan and Dr. Rucsandra Moldovan for their consistent support, guidance, encouragement, and mentorship during my Ph.D. journey. I am very grateful to them and proud to be their student. I would also like to express my sincere gratitude to my dissertation committee member, Dr. Dongyoung Lee, my examiner Dr. Elisabeth Peltier, and my external examiner Dr. Lyne Bouchard for their time reviewing my thesis and for their insightful and constructive feedback and advice on my research. My thesis completion would not have been possible without their guidance and support.

This work would not have been possible without the financial support of the Social Science and Humanities Research Council (SSHRC) and of the Stephen A. Jarislowsky Chair in Corporate Governance and the Institute for the Governance of Private and Public Organizations. I also thank all faculty members, colleagues, and friends who supported me throughout my Ph.D. journey.

It goes without saying that my deepest gratitude goes to my parents Alireza Amani and Maryiam Amani and the rest of my family (especially my sister Parvaneh) for lifting me throughout this incredible journey. I cannot find enough words to thank them, other than humbly dedicating this achievement to them as token of gratitude and appreciation. I promise to continue to do my best and always make them proud.

**Table of Contents**

## Chapter 1: Introduction

Cybersecurity risk is a major global problem, among the risks of highest likelihood in the coming years (World Economic Forum 2021), and one of the "most worrisome" issues faced by organizations (Kappelman et al. 2020) as they amass huge amounts of electronic data (Lieberman 2017). Cybersecurity breaches continue to accelerate in frequency, severity, and impact. In 2022, average data breach costs were at their highest in the last 17 years, rising from USD 4.24 million in 2021 to USD 4.35 million in 2022 (IBM 2022). Organizations currently allocate more than USD 150 billion annually towards cybersecurity, a figure that is expected to exceed USD 200 billion by 2025 (Gartner 2021).

At the organizational level, a successful cyber-attack can cause loss of market value and reputation, increase cost of capital and audit fees, lead to regulatory scrutiny and/or litigation, and compromise corporate intellectual property and clients' data (Banker and Feng 2019; Frank et al. 2021; Huang and Wang 2021; Li et al. 2020). Beyond a single organization, such attacks can impact various market participants including breached firms (Kamiya et al. 2021), suppliers (He et al. 2020), peer and non-peer firms (Ashraf 2021), customers (Martin et al. 2017), and investors (Campbell et al. 2003). At a more macroeconomic level, the impact of data breaches can be far reaching as it spreads through firms' supply chains (Crosignani et al. 2023), extends to the financial infrastructure (Kopp et al. 2017), and the overall economy (Eisenbach et al. 2022).

Considering the significance of and increase in cybersecurity risks and incidents, investor groups place increasing pressure on corporate boards to prioritize cybersecurity risk oversight and management (Davis 2016), particularly since a substantial proportion of data breach costs is borne by investors (Clayton 2017). In addition to investor demands, over the past decade, a number of laws, regulations, and guidance have been introduced calling organizations to provide high-quality

disclosure on cybersecurity risks and incidents (e.g., Securities and Exchange Commission (henceforth, SEC) 2011 and 2018 guidance; data privacy laws; data security laws; data breach notification laws; and industry-specific regulations). Currently, the SEC is reviewing a new proposed rule that seeks to improve public companies' disclosures of cybersecurity risk management, strategy, governance, and incident reporting (SEC 2022). The increased number of cybersecurity incidents (IBM 2022), extensive media coverage (Verizon Enterprise Solutions 2015), and intense scrutiny of firms' cybersecurity risks and incidents reporting practices further highlight the importance of effective disclosure. In particular, professional publications report that cybersecurity disclosure is insufficient, with 65% (90%) of known cyberattacks in public firms between 2011 and 2017 (2018) remaining undisclosed in firms' SEC filings (Coleman 2018; Rubin 2019).

In light of these developments, it is important to provide researchers, practitioners, regulators, and other stakeholders with information about the current state of research on cybersecurity risks and incidents disclosure (the focus of the first essay). In addition, considering the growing pressure from investor, media, regulators, and other stakeholders, there is more and more interest in effective cybersecurity risk governance (the focus of the second essay) and management (the focus of the third essay).

The first essay systematically compiles and reviews the research on cybersecurity risks and incidents disclosure, identifies trends and patterns, and offers suggestions for future research. Thus, the objective of this essay is to answer the following research questions with respect to cybersecurity risks and incidents disclosure: 1) what are its determinants? 2) is it informative? 3) what is the current state of its content and quality? 4) what are its theoretical perspectives, methods,

disclosure outlets, and data sources used in the literature that examines this type of disclosure? and 5) what future research venues emerge from the review of the current literature?

The bulk of research in cybersecurity focuses on its technical aspects, yet cybersecurity risks and incidents also have a profound impact from an accounting perspective. The expertise of accountants contributes to managing cybersecurity risks by testing controls and mitigating cyber exposure, while also assessing the costs of cyber incidents, tracking their effect on a firm's performance, and ensuring transparent disclosure to stakeholders (Eaton et al. 2019; Janvrin and Wang 2022). For instance, while internal auditors can offer assurance on information security and insights on improving the firm's cybersecurity practices (Steinbart et al. 2012; 2018), external auditors adjust their risk assessment and audit procedures based on the firm's cybersecurity risks and incidents disclosure (Li et al. 2020).

From a theoretical perspective, disclosure of cybersecurity risks and incidents can be viewed from the point of view of agency theory that focuses on how information asymmetry could be reduced in such situations (Jensen and Meckling 1976) or signaling theory that focuses on conveying firms' commitment to cybersecurity (Spence 1973) and avoiding the litigation and reputational damages (Skinner 1994). However, disclosure without careful consideration and proper cost-benefit analysis (Verrecchia 1983) may lead to a firm being exposed to cybersecurity attacks that can jeopardize its operations. Nevertheless, the existence of managerial opportunistic behavior (Beyer et al. 2010) and managerial discretion with respect to cybersecurity disclosure is also a dimension that should be considered.

Recently, cybersecurity issues have been tackled from accounting perspectives. Hence, the essay follows the three stages (planning, conducting, and reporting) for conducting a systematic literature review (Kitchenham and Charters 2007) and develops the main corpus of papers by an

automated keyword search of digital sources for the term "*disclosure*" and cyber-related terms. A careful reading of paper titles and abstracts identifies 28 relevant papers, which are supplemented by a snowball technique that includes 13 additional papers, resulting in a final selection of 41 papers for the review.

The synthesis of these 41 papers reveals the following. First, prior studies' results suggest the existence of multiple factors that motivate firms to disclose information pertaining to cybersecurity risks and incidents. These factors include pressure from regulators and the public, characteristics of board governance (namely, board expertise and gender diversity), of the firm (namely, size, profitability, intangibility, and industry sector), and of the cyber incident (namely, severity and recurrence).

Second, prior studies' results reveal that, while the level of informativeness of cybersecurity disclosure meets the expectations of regulators, the quality of such disclosure falls short of regulatory expectations. More specifically, the former highlights informativeness of disclosures of cybersecurity risks, risk management activities, and cyber incidents, and the latter indicates that cybersecurity disclosure is boilerplate, not unique, less readable, more litigious, and with limited level of detail and completeness. These results may be explained by firms attempting to balance regulatory requirements and guarding against litigation and further breach exposure risks.

Third, most studies on cybersecurity disclosure lack an explicit theoretical framework, often relying on assumptions from prior literature, which may lead to findings that are not grounded in theoretical foundations (hence maybe incomplete and/or inaccurate). Moreover, the most researched disclosure outlets, as expected, are annual reports, a sub-section thereof, and 8-K

reports; and the most common methodologies are textual and content analysis as well as event studies. Only a few studies use qualitative research methods.

Finally, the review identifies important research gaps and potential future directions. For example, the current research examines limited governance characteristics such as board gender diversity and board expertise with prior breaches. The second essay in this thesis aims to contribute to this line of research by exploring other board governance characteristics and structures as drivers of cybersecurity governance disclosure practices. As the issue of cybersecurity continues to gain prominence, there has been an increasing interest among investors, regulators, and other stakeholders to gain insight into the measures that organizations are implementing as part of their risk management strategy to protect against, prepare for, and manage cybersecurity incidents. The third essay in this thesis adds to this literature by examining firms' disclosure of cybersecurity risk transfer via cyber insurance.

Other potential areas of research that the first essay identifies are exploring the informativeness of cybersecurity risks and incidents disclosure beyond equity market including debt, cybersecurity, and cyber insurance markets; examining not only the syntactic features but also the semantic dimensions and how these characteristics vary across different disclosure outlets; and investigating the relationship between variations in cybersecurity risks and incidents disclosure across firm and country characteristics. Overall, the first essay identified the main gaps of the current cybersecurity disclosure literature and opportunities for future research.

Effective governance is necessary considering pressures exerted by investors, regulators, and other stakeholders and that governance implications of cybersecurity risks are not fully understood (Rajgopal and Srinivasan 2016). Thus, the second essay examines the governance of cybersecurity risks through the lens of board cybersecurity risk oversight responsibility. Focusing

on board cybersecurity risk oversight is crucial as it sets the "tone at the top", thus influencing organizational cybersecurity culture, providing legitimacy for risk management, and steering employee compliance and sense of accountability towards cybersecurity risk practices (Beasley et al. 2022; Braumann et al. 2020; Maurer et al. 2021). In addition, the SEC stipulates that overall risk oversight is the responsibility of the board (SEC 2009).

Hence, the objective of the second essay is three-fold: 1) examine who has governance responsibility to oversee cybersecurity risk, 2) seek to identify the key governance determinants of cybersecurity risk oversight, analyzing how these determinants may vary across different oversight setups, and 3) explore the effectiveness of firms' cybersecurity risk oversight by examining the relationship between a firm's oversight setup and its response to a cybersecurity breach incident.

The SEC issued cybersecurity disclosure guidance in 2011 and 2018 to assist publicly traded companies in preparing and reporting their cybersecurity disclosures (SEC 2011; 2018) and is reviewing a proposed rule requiring disclosures about board of directors' oversight of cybersecurity risk (SEC 2022). All 50 U.S. states and many countries have enacted cybersecurity regulations, and additionally numerous professional organizations issued cybersecurity-related guidelines and frameworks. Despite these measures, the SEC has not taken a position on cybersecurity risk oversight responsibility assignment (Loop 2016), leaving it to each entity to determine to whom it assigns such responsibility. Given such discretion, cybersecurity risk oversight still struggles to find a home in the boardroom (PwC 2018).

From a theoretical perspective, the efficiency-based view argues that the full board should oversee cybersecurity risk and not delegate it to a board-level committee (Rothrock et al. 2018), for cost considerations or to avoid the perception that the board lacks appropriate expertise (Higgs

et al. 2016; Jewer and McKay 2012). The competency-based view offers a different perspective and argues that there are factors that constrain the full board involvement in the oversight, leading the board to delegate this responsibility to a board-level committee (Price and Lankton 2018). According to this view, factors impeding full board involvement in cybersecurity oversight include low information technology (IT) knowledge and experience among board members (Turel and Bart 2014), inadequate recognition of IT's strategic importance within the organization (Nolan and McFarlan 2005), and the potential benefits of a dedicated board-level committee(s) for rigorous monitoring and evaluation of cybersecurity risks.

Using a combination of textual analysis of firms' proxy statements (DEF 14A), with manual extraction of oversight assignment, and breach events from Advisen Ltd. (Cyber Loss Data, a proprietary dataset) during 2010-2020, this essay examines whether boards oversee cybersecurity risk directly or assign it to a board-level committee(s). The analysis reveals that most firms do not disclose the board's role in cybersecurity risk oversight in their proxy statements. Shortly after the SEC 2011 cybersecurity guidance, firms started to increasingly disclose assignment of cybersecurity oversight, with 84 percent, among those who explicitly disclose oversight, assigning it to a board-level committee(s) and 16 percent to the full board.

Exploratory analysis also shows variation in board-level committee(s) assignment across industry sectors, including committees for audit, finance, technology, compliance, risk, cybersecurity, nominating and governance, and other or to a joint committee. Nevertheless, a majority of firms choose to entrust oversight responsibility to the audit committee, risk committee, or technology committee. Moreover, a small proportion of firms, accounting for five percent of the total, shift the oversight responsibility from a board or board committee(s) to another.

Building on the insights gained from analyzing cybersecurity risk governance responsibility, the next set of analyses turns to the governance determinants of oversight using a cascading three-level analysis approach. To achieve that, and for simplicity, the analysis groups oversight responsibility into three categories, specifically, full board, audit committee, and non-audit board-level committee(s).

The essay identifies the board's cyber competency, network size, equity holding, and gender diversity as significant determinants of disclosing cybersecurity oversight responsibility. The results also reveal that while the board's cyber competency and network size positively contribute to the assignment, equity ownership and gender diversity exhibit a negative impact. Additionally, the presence of a cybersecurity role and a risk management framework at the management level plays an important role in determining oversight responsibility assignment. Furthermore, the findings indicate that full boards oversee cybersecurity risk in firms with smaller boards.

The essay further suggests that boards with greater equity ownership and cyber experience are inclined to delegate oversight to the audit committee, whereas larger boards with a wider network size are inclined to delegate it to a non-audit board-level committee(s). Finally, the essay highlights the audit committee is the default option for delegating the responsibility for cybersecurity risk oversight in organizations with existing risk, compliance, and/or technology committees.

Focusing on the last research question on the consequences of a cybersecurity breach event, the essay examines the effects of having oversight (and who has responsibility for such oversight) on how firms react to a cybersecurity breach incident. Specifically, the essay focuses on breach events where a firm has explicitly indicated its oversight responsibility assignment before the

breach incident. By examining three variables – time to the breach announcement, time to the breach resolution, and the frequency of a breach – the findings indicate that the presence of oversight, on average, reduces the duration of time it takes for firms to declare the breach and the duration of time required to rectify the breach. Moreover, cybersecurity oversight reduces the occurrence of such breaches. Hence, explicitly assigning cybersecurity oversight responsibility provides tangible economic benefits to a firm. Further analysis indicates that audit committee oversight is more effective for the promptness of breach announcement and resolution, whereas full board oversight is more effective in reducing the frequency of such breaches. Overall, these findings are robust to alternative sample matching techniques.

Given the increasing pressures from investors, regulators, and other stakeholders, there is a need to proactively manage cybersecurity risks (Sonnemaker 2019). Hence, the third essay examines the relation between firms disclosing their cyber insurance and the likelihood of a data breach as well as the relation between firms disclosing their cyber insurance and breach consequences.

The significance of cyber insurance is highlighted by the US market's value of over USD 3 billion annually, projected to grow two to seven times in the next decade (PwC 2021; Coker 2021). In addition, cyber insurance is crucial for firms' cybersecurity risk management policies, compliance with federal securities laws (SEC 2018), reliable financial reporting (Cohen et al. 2017), and for motivating organizations to increase preventive investments (Panda et al. 2021). Knowledge of cyber insurance can also contribute to the development of new cybersecurity regulations (Hobson and Adams 2020).

Firms may use cyber insurance to enhance cybersecurity, reduce data breach costs, and access insurance providers' expertise and services (Boyer 2014; Frank et al. 2021; Mittel, 2020;

Talesh 2018). However, underestimating its importance and concerns of false sense of control and high premiums (Eling and Schnell 2016; Kshetri 2020) can hinder its effectiveness. Additionally, coverage scope and estimating attack probability and losses pose challenges for clients in the emerging cyber insurance market (Francis et al. 2021; Koijen and Yogo 2022).

Firms may disclose cyber insurance coverage to signal commitment to cybersecurity and risk management (Gordon et al. 2010), and to reduce information asymmetry with capital markets (Jensen and Meckling 1976). However, such disclosure may attract unwanted attention from hackers, reducing incentives to disclose. Thus, the relationship between the joint probability of having cyber insurance and disclosing it and the likelihood of breaches is an empirical question.

Using 10-K filings' "Item 1A. Risk Factors" section from 2010-2021, a two-stage textual analysis identifies and searches for key terms that proxy for cyber insurance disclosure. Combining these with Advisen Ltd.'s proprietary dataset on cyber breach status, the analysis shows that disclosing cyber insurance increases the likelihood of a breach event by 51 percent. This finding suggests that hackers may be attracted to disclosed cyber insurance, or insured firms may not prioritize safeguarding against cyber breaches, or both. This inference holds not only across financial and non-financial sectors, but also when using alternative approaches including a propensity score matching, two stage least squares with instrumental variables, and Heckman (1979) two-stage model.

Next, the essay examines the effectiveness of cyber insurance in the event of an actual cyber breach, namely the association between disclosure of cyber insurance and the timeliness of breach announcement, resolution, and its frequency. The essay argues that while cyber insurance may accelerate the announcement and resolution of breaches by providing access to incident response, communication, and legal expertise (Talesh 2018), it may also prolong the process by

requiring time-consuming investigations to determine policy coverage and liability. As for breach frequency, the essay argues that while cyber insurance may decrease a firm's exposure to breaches by evaluating their security measures and bridging cybersecurity knowledge gaps, it may not decrease the frequency of cyber incidents as it draws cybercriminals' attention (Cimpanu 2020; Havakhor et al. 2020) and reduces incentives for self-protection (Eling and Schnell 2016).

The essay finds that firms disclosing cyber insurance experience mixed results in the event of a breach. While they take longer on average to disclose the breach, cyber insurance helps reduce the time to resolve the breach. The delay in breach announcement may be due to firms not fully leveraging the expertise of their insurance providers or to the time required to access such expertise. Conversely, the quick resolution of the breach is attributed to the insurance providers' expert handling of the aftermath. Results also show a positive association between cyber insurance and breach frequency, supporting the argument that disclosing cyber insurance may expose firms to become targets of future attacks.

The rest of the dissertation is organized as follows. The next three chapters present each of the three essays. The fifth chapter concludes.

## Chapter 2: Cybersecurity Risks and Incidents Disclosure: A Literature Review


### Abstract

The increasing prevalence of cybersecurity risks and incidents, coupled with a multitude of pressures from different stakeholders, highlights the importance of their disclosure. This review synthesizes literature on cybersecurity risks and incidents disclosure to identify its drivers, informativeness, quality, and theoretical perspectives. This paper conducts a systematic cybersecurity disclosure literature review, analyzes the relevant papers through summarization, categorization, and comparison, and synthesizes the results to address the research questions. The review identifies various drivers for cybersecurity disclosure, highlights that while the level of informativeness of such disclosure meets the usefulness expectations of regulators, its quality falls short. Most studies lack an explicit theoretical framework and use predominantly textual content analysis and event studies. The synthesis informs regulators, executives, and capital market participants of the need for closer attention to the quality and informativeness of cybersecurity disclosure and to the drivers that may help in this regard. This is the first literature analysis dedicated to cybersecurity disclosure with significant implications for research and practice. It synthesizes drivers, informativeness, quality, and theoretical underpinnings of cybersecurity disclosure.



**Keywords:** Literature review, disclosure, cybersecurity risks and incidents


### 2.1 Introduction

Over the past decade, a substantial number of laws, regulations, and guidances have emerged calling organizations for quality cybersecurity risks and incidents disclosure (e.g., Securities and Exchange Commission (SEC), 2011, 2018; data privacy laws; data security laws;

and breach notification laws; industry-specific regulations).[1,2] The increased number of cybersecurity incidents (IBM 2022), extensive media coverage (Verizon Enterprise Solutions 2015), and intense scrutiny of firms' cybersecurity risks and incidents reporting practices further highlight the importance of this topic. In addition, the complexities and unique features of cybersecurity events, as well as the need to reduce information asymmetry among various stakeholders and organizations, all contributed to a growing body of cybersecurity risks and incidents reporting literature.

This study compiles and reviews research on cybersecurity risks and incidents disclosure, identifies trends and patterns, and offers suggestions for future research. It complements as well as extends previous reviews such as Haapamäki and Sihvonen (2019), Spanos and Angelis (2016), and Walton et al. (2020). More specifically, the objective of this literature review is to answer the following research questions: 1) What are the determinants that motivate firms, as part of their risk strategy, to disclose cybersecurity risks and incidents? 2) Are disclosure of cybersecurity risks and incidents informative? 3) What is the current state of the content and quality of cybersecurity risks and incidents disclosure? 4) What theoretical perspectives, methods, disclosure outlets, and data sources do research into cybersecurity risks and incidents use? and 5) What future research venues emerge from the review of the current literature?

Cybersecurity risks and incidents can have a profound impact on accounting for several reasons. Firstly, the expertise of accountants greatly contributes to the management of

[1] National Initiative for Cybersecurity Careers and Studies (NICCS) (2022) defines *cybersecurity* as "the activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation" and *cyber incident* as "an occurrence that actually or potentially results in adverse consequences to (adverse effects on) (poses a threat to) an information system or the information that the system processes, stores, or transmits and that may require a response action to mitigate the consequences".

[2] The phrase "cybersecurity risks and incidents disclosure" is from SEC guidance (2011, 2018). Throughout the paper this phrase is used interchangeably with the phrase "cybersecurity disclosure".

cybersecurity risk through the identification, prioritization, and testing of controls, as well as the mitigation of cyber exposure and provision of reporting and assurance services (Eaton et al. 2019). Furthermore, in the event of cyber incidents, accountants play a critical part in assessing the costs of these incidents and tracking their effect on a firm's performance and ensuring that these incidents are communicated to investors and other stakeholders in a transparent and appropriate manner (Janvrin and Wang 2022). Also, while internal auditors can offer assurance on information security and insights on improving the firm's cybersecurity practices (Steinbart et al. 2012; 2018), external auditors adjust their risk assessment and audit procedures based on the firm's cybersecurity risks and incidents disclosure (Li et al. 2020).

Several factors motivate this review. First, cybersecurity risk is a major global problem and is among the risks of highest likelihood in the coming years (World Economic Forum 2021), and one of the "most worrisome" issues faced by organizations (Kappelman et al. 2020), given the inherent ambiguity and complexities of its cost-benefit analysis, where the certainty and costs are relatively easier to quantify than the benefits (Gansler and Lucyshyn 2005). Second, cybersecurity events differ from other corporate events such as earnings announcements, management forecasts, or repurchases on several dimensions. For instance, their timing is unpredictable (possibly random), nonperiodic, and they have relatively higher frequency and faster spread (Crosignani et al. 2023) than other corporate events. Cybersecurity events are also largely idiosyncratic in that they "do not specifically affect the quality of the products or services offered by the affected company" (Akey et al. 2021). Furthermore, they result in major losses for various market participants including breached firms (Huang and Wang 2021; Kamiya et al. 2021), suppliers (He et al. 2020), peer (non-peer) firms (Ashraf 2021), customers (Martin et al. 2017), investors. Not only that, but their impact can be far reaching propagating through firms' supply chains

(Crosignani et al. 2023) and extends to the financial infrastructure (Kopp et al. 2017) as well as the aggregate economy (Eisenbach et al. 2022).

Third, the dynamic nature of cybersecurity, organizations full reliance on the internet, and directors' relative illiteracy about cybersecurity may lead to "underestimation of risk, confirmation bias, aspiration-based risk taking, and overconfidence" (Sumner et al. 2020). Fourth, professional publications report that cybersecurity disclosure is insufficient, with 65% (90%) of known cyberattacks in public firms between 2011 and 2017 (2018) remaining undisclosed in filings to the SEC (Coleman 2018; Rubin 2019).[3] Not only that, but when such events are disclosed, there are variations in the method and substance of their disclosure (Coleman 2018).

Finally, the disclosure of cybersecurity risks and incidents faces numerous multifaceted tensions. For example, the persistent debate and ongoing research efforts surrounding the incentives for managers to voluntarily report negative information (Campbell et al. 2014), such as cybersecurity risks and incidents disclosure, especially since such disclosure is not mandatory. Furthermore, the limited availability of a firm's cybersecurity related information outside of the firm's reporting complicates the disclosure tension. Moreover, the existence of managerial opportunistic behavior (Beyer et al. 2010) and the managerial discretion with respect to cybersecurity risks and incidents disclosure further exacerbates the difficulty of the situation. Finally, the challenge of providing meaningful cybersecurity information while minimizing the firm's vulnerability to cyberattacks requires careful consideration to reduce information asymmetry (Jensen and Meckling 1976), signal (Spence 1973) the firm's cybersecurity posture, mitigate the costs of litigation and reputational damage (Skinner 1994), and avoid disclosing

[3] Facebook Inc. discloses via blog about a breach of its 50 million user accounts without disclosing in regulatory filings (Rubin 2019).

sensitive (Verrecchia 1983) cybersecurity information to prevent potential hackers from penetrating the firm's security.

Several findings arise from the synthesis of prior research. First, prior studies' results suggest the existence of multiple factors that motivate firms to disclose information pertaining to cybersecurity risks and incidents. These factors include regulatory pressure, public pressure, institutional pressure, board governance and firm characteristics, and characteristics of a cyber incident. Second, the existing literature on the topic of cybersecurity disclosure reveals that, while the level of informativeness of such disclosures meets the expectations of regulators in terms of usefulness, the quality of such disclosures falls short of regulatory expectations as evidenced by studies on the content and quality of cybersecurity disclosure. Third, most studies on cybersecurity disclosure lack an explicit theoretical framework, often relying on assumptions from prior literature. Moreover, the most researched disclosure outlets, as expected, are annual reports, followed by specific section of the annual reports, and 8-k reports, while conference calls and social media are the least used outlets. Finally, the most used methodologies are textual and content analysis as well as event studies. Only a few studies use qualitative methods.

This systematic literature review provides the following contributions to research and practice. First, this study provides an up-to-date review of the cybersecurity risks and incidents disclosure literature, summarizing data sources, methodological approaches, theoretical lenses while presenting venues for future research. Considering the rapid technological, regulatory, and legal developments underlying cybersecurity events, it is critical to keep a timely understanding of their disclosure. This literature review establishes that prior research is mainly empirical in nature and does not explicitly include theories; but rather focuses on textual analysis of annual reports or sections thereof with the majority adopting quantitative approaches. Thus, the review

elucidates the state of the narrative sections of corporate filings, thus expanding extant literature on narrative disclosures and content analysis (Li 2010; Loughran and McDonald 2016).

Second, this review complements the recent work of Haapamäki and Sihvonen (2019) and Walton et al. (2020), who both identify cybersecurity risks disclosure as one of the themes in their cybersecurity literature reviews. While Haapamäki and Sihvonen (2019) have only five papers on this theme within the context of accounting and auditing literature, Walton et al. (2020) add six more papers based on a multi-discipline literature context. However, this review differs from both reviews in breadth in that it uses a search set that combines the key terms of both reviews, and in recency in that it covers three years beyond their timeframe coverage, adding 25 more papers. Hence, the review expands the coverage of their cybersecurity disclosure theme by evaluating the relevant literature more extensively and incorporating more components of this theme, consequently, broadening our understanding of this core topic. More specifically, the review provides insights on cybersecurity risks and incidents disclosure components including determinants, informativeness, content and quality, and theoretical frameworks used, which offers opportunities for future granular research on cybersecurity disclosure.

Finally, this review highlights not only the reporting practices of cybersecurity disclosure with respect to risks and incidents, but also the preventive and mitigation practices and measures used to address such risks and incidents. In addition, the review provides practitioners with factors that motivate firms to disclose their cybersecurity risks, which may enable them to devise strategies that increase the overall level and transparency of cybersecurity risks and incidents reporting without increasing their vulnerability and exposure. Thus, the practical usefulness of cybersecurity risks and incidents disclosure to enhance a firm's cybersecurity posture stems from formulating a corporate disclosure policy that incorporates a combination of multiple dimensions. Particularly,

cybersecurity disclosure needs to reflect the proper drivers of the disclosure as well as the quality of such disclosure, to balance standardization and firm specificity, to comply with both local and international regulations, and to accommodate the needs of various stakeholders. The limitations in both the content and quality of cybersecurity disclosure call for better compliance with the guidance to improve such disclosure as well as more monitoring attention from regulators.

The rest of the paper is organized as follows. Section 2 provides the institutional background for cybersecurity disclosure and prior cybersecurity literature review. Section 3 presents this study review methodology. Section 4 provides synthesis of prior studies. Section 5 highlights future opportunities, and Section 6 concludes.

## 2.2 Background

### 2.2.1 Institutional perspective

All organizations, whether regulated or not, are generally subject to legal duties pertaining to their corporate data, which include (1) the duty to protect the security of such data, and (2) the duty to disclose data breaches when they occur (Smedinghoff 2015). The following section summarizes the various cybersecurity risks and incidents disclosure obligations and public reporting requirements.

#### *2.2.1.1 Cybersecurity guidances*

At the beginning of 2005, the SEC started requiring corporations through Regulation S–K, Item 305(c) to include material risk information under item 1A (i.e., Risk Factor Disclosure) in their 10-K filings (SEC 2005). However, the mandate was not explicit about disclosure of cybersecurity risks and incidents.[4] The increasing number of publicized cybersecurity attacks at

[4] This matter stayed the same even after SEC's modernization of Regulation S-K Items 101, 103, and 105 (SEC 2020a; 2020b). Specifically, the SEC in 2020, amended the Risk Factors disclosures requirements to reflect a more principles-based approach by only requiring disclosure of "material" risk factors, and "[c]onsistent with this principles-based

the beginning of 2011, prompted the SEC Division of Corporation Finance in 2011 to issue a new disclosure guideline. This guidance instructs corporations about disclosure obligations relating to cybersecurity risks and incidents in their SEC regulatory filings. Although, the "guidance is not a rule, regulation, or statement" of the SEC (SEC 2011), it has been given "the de facto effect of law" (Ferraro 2013).[5] The SEC requires disclosure of cybersecurity risks and incidents in the following 10-K sections (1) risk factors, (2) management's discussion and analysis (MD&A) of financial condition and results of operations, (3) description of business, (4) legal proceedings, (5) financial statement disclosures, and (6) controls and procedures. As 2011 guidance mentions, "no existing disclosure requirement explicitly refers to cybersecurity risks and incidents, a number of disclosure requirements may impose an obligation on registrants to disclose such risks and incidents" and companies need to "provide disclosure tailored to their particular circumstances and avoid generic "boilerplate" disclosure, we reiterate that the federal securities laws do not require disclosure that itself would compromise a registrant's cybersecurity" (SEC 2011). Hence, firms have discretion in deciding whether, what, and how much to disclose.

In 2018, the SEC issued an updated interpretive guidance to assist public companies in preparing and reporting their cybersecurity disclosures to investors (SEC 2018). This interpretive guidance, which reinforces and expands on the SEC 2011 guidance, addresses two new topics "namely the importance of cybersecurity policies and procedures and the application of insider trading prohibitions in the cybersecurity context" (SEC 2018). Overall, the SEC 2011 guidance

approach, we are not adding a specific requirement to disclose cybersecurity risk as recommended by a commenter" (SEC 2020a).

[5] Based on analysis of SEC comment letters to 50 registrants requesting additional information about their cyber incidents and the registrants' subsequent correspondence, Ferraro (2013) concludes that the guidance "has been given the de facto effect of law" as the registrants did not have a choice but to disclose more information about their cybersecurity attacks; despite the registrants' claims of immateriality of such attacks.

and 2018 interpretive guidance are not only calling for greater awareness for cybersecurity disclosures but also highlighting SEC expectation for such disclosures.

The SEC is currently reviewing a new proposal rule that seeks to standardize and improve the public companies' disclosures regarding their cybersecurity risk management, strategy, governance, and cybersecurity incident reporting (SEC 2022). Moreover, the proposed rule is expected to require public companies to make periodic disclosures about their policies and procedures for identifying and managing cybersecurity risks, the role of management in implementing these policies and procedures, and the board of directors' cybersecurity expertise and its oversight of cybersecurity risk.

#### *2.2.1.2 Industry specific regulations*

In addition to the SEC, the Federal Trade Commission and other government agencies impose industry-specific data security regulations. Organizations in the healthcare sector, for example, must comply with the Health Insurance Portability and Accountability Act (HIPAA) and HIPAA Security Regulations, while organizations in the financial sector must comply with the Gramm-Leach-Bliley Act (GLB). Furthermore, the federal government sector and the critical infrastructure sectors are also subject to stringent data security regulations.

#### *2.2.1.3 State-level information-security and data-breach notification laws*

Organizations are also subject to a variety of state laws that require the implementation of security measures to protect corporate data, such as the California Consumer Privacy Act, the Utah Consumer Privacy Act, Massachusetts data security regulations, and others. The legal obligation to disclose security breaches to the persons affected stems from data breach notification laws - all

50 U.S. states have issued such laws.[6] These data breach notification laws differ in terms of the definitions of data breaches and personal data, penalties, content of data breach notifications, notice to consumers of data breaches, and notices to a supervisory body of data breaches.

#### *2.2.1.4 Global regulations*

Although many countries around the world have passed data privacy laws, including Canada, Australia, and Japan, a more far-reaching law is the 2018 European Union (EU) General Data Protection Regulation (GDPR) which applies to organizations that store or process personal data about EU residents regardless of the organization's domicile.

#### *2.2.1.5 Professional bodies*

Many professional organizations issued policies, procedures, guidances, and frameworks related to cybersecurity risks. For example, the Public Company Accounting Oversight Board (PCAOB) and the Center for Audit Quality (CAQ) have provided tools and resources to board of director members in identifying potential cybersecurity risks (PCAOB 2018; CAQ 2018). In 2017, the American Institute of Certified Public Accountants (AICPA) issued Cybersecurity Risk Management Framework that provides organizations criteria to evaluate their cybersecurity controls and communicate and manage information about their cybersecurity risk to interested parties (AICPA 2017a; 2017b). Moreover, the AICPA issued documents that provide tools to the board members on how to effectively discuss cybersecurity risks and disclosures with management and CPA firms (AICPA 2018).

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) has issued a new guidance on managing cyber risks in a digital age (COSO 2015). The guidance explains how companies can apply COSO's Enterprise Risk Management to manage cyber risks

[6] See National Conference of State Legislatures (2020) for a summary and Congressional Research Service (2019) for further information on breach-reporting requirements.

and protect organizations against cyberattacks. In addition, the Institute of Internal Auditors (IIA) also issued a practice guide that discusses the internal audit activity's role in cybersecurity and how to provide assurance over cybersecurity risks (IIA 2016). Furthermore, the Institute of Risk Management (IRM) issued a report and practical guidance, which explores risk management in the context of cyber risk (IRM 2014a; 2014b). There are other well-known cyber-focused standards and IT governance frameworks that provide conceptual roadmaps such as COBIT 2019, ISO/IEC 27002, and National Institute of Standards and Technology (NIST) Cybersecurity Framework (ISACA 2021; ISO 2013; NIST 2018).

### 2.2.2 Prior cybersecurity literature

Extant literature on cybersecurity literature generally provides a review from a specific discipline(s) (Haapamäki and Sihvonen 2019; Walton et al. 2020) or focuses on a specific aspect of cybersecurity (Richardson et al. 2019; Spanos and Angelis 2016). Haapamäki and Sihvonen (2019) synthesize a total of 39 theoretical and empirical cybersecurity studies published in accounting and auditing literature. The authors identify five research themes namely 1) cybersecurity and information sharing, 2) cybersecurity investments, 3) internal auditing and controls related to cybersecurity, 4) disclosure of cybersecurity activities, and 5) security threats and security breaches. Without restriction on disciplines, Walton et al. (2020) review 68 cybersecurity papers in the accounting, information systems, computer science, and general business disciplines. The review integrates and classifies papers also into five categories including 1) cybersecurity risk disclosure, 2) cybersecurity investment, 3) information security governance, 4) market response to cybersecurity incidents and spillover effect, and 5) manager, auditor, and customer responses, and remedial strategies. The two reviews are broadly identical in their

synthesized research themes. The focus of this review is specifically on the cybersecurity risks and incidents disclosure theme.

Another stream of reviews focuses on specific aspects of cybersecurity, namely while Spanos and Angelis (2016) conduct a systematic literature review of the stock market reaction to disclosure of information security events, the Richardson et al. (2019) review focuses on a broader economic consequences including stock market reaction, accounting performance measures, audit and other fees, and internal control material weaknesses. Furthermore, the Cram et al. (2019) review focuses on research relating to cybersecurity policies, and the Janvrin and Wang (2022) review focuses on developing an Event, Impact, Response Framework to explore the influence of cybersecurity on accounting. This study is similar to these reviews in the sense that it focuses on a specific aspect of cybersecurity, namely disclosure with elaborate coverage of this central aspect.

### 2.3. Methodology

The study follows the guidelines of Kitchenham and Charters (2007) the three stages (planning, conducting, and reporting) for conducting a systematic literature review.[7] The planning stage involves the identification of the need for the systematic literature review and the development of the review protocol. For the need, it is important to provide researchers, practitioners, regulators, and other stakeholders with information about the current state of cybersecurity risks and incidents disclosure research given the evolving and dynamic nature of such risks. Furthermore, although there are studies that provide literature reviews on cybersecurity, these studies either focus on a specific discipline(s) or other aspects of cybersecurity, none of these studies has specifically provided a systematic review of cybersecurity risk and incidents disclosure, which is the focus of this study.

[7] Although these stages appear to be sequential, these stages involve many iterations.

The review protocol sets procedures for the conducting stage and aims to answer the following research questions: 1) What are the determinants that motivate firms to disclose cybersecurity risks and incidents? 2) Are disclosure of cybersecurity risks and incidents informative? 3) What is the current state of the content and quality of cybersecurity risks and incidents disclosure? 4) What theoretical perspectives, methods, and data sources researchers into cybersecurity risks and incidents disclosure use? and 5) What are identifiable research gaps and potential future directions of cybersecurity risks disclosure? To develop the main corpus of papers pertinent to the study, an automated keyword search (within the titles, abstracts, and keywords of the papers) of two main digital sources (Scopus and Business Source Ultimate) is performed using the term "*disclosure*" and the following terms from Haapamäki and Sihvonen (2019) and Walton et al. (2020):[8]

> "disclosure" and ["cybersecurity" or "cyber" or "security threats" or "cyber threats" or "cyber-attack" or "information breach" or "data breach" or "data theft" or "information security" or "data security" or "IT security" or "security breach"]

The study's inclusion/exclusion selection criteria are limited to papers that focus on cybersecurity disclosure within a business context with no specific time restrictions. Figure 1 presents the steps to create the main corpus of papers. The initial search produces 7268 papers, and 6796 papers are removed that are either irrelevant or duplicate. Careful reading of paper titles and abstracts of 472 results in 28 relevant papers. To complement and enrich the literature, a snowball technique is also incorporated and consequently, 13 papers are added based on the references of articles selected from prior steps. Thus, the final number of papers used in this review is 41 papers.

[8] Massaro et al. (2016) supports that "to investigate an emerging field for which little literature exists. In this case, keyword searches are paramount because they identify recently published articles".

The conducting stage entails reading carefully and critically and constructively analyzing papers through summarization, comparison, and categorization. In particular, the units of analysis of the review encompass data features including authors, year of publication, research objective(s), theory used, methodology employed, and the main findings.

…….. [Insert Figure 1 about here] ……..……...

**2.4. Discussion and synthesis**

Table 1 presents a summary of reviewed papers. The summary reports the author(s), journal title, the research objective(s), and the main findings. The following sections elaborate on literature relevant to each research question.[9]

…….. [Insert Table 1 about here] ……..……...

**2.4.1. Determinants of cybersecurity disclosure**

The synthesis of the literature reveals multiple drivers that motivate firms to disclose cybersecurity risks and incidents. In the context of regulatory pressure, Gordon et al. (2006) find that firms increase emphasis on information security activities disclosure after passage of Sarbanes-Oxley Act, others report increase of cybersecurity disclosure in 10-K filings post SEC 2011 guidance (Gao et al. 2020; Hilary et al. 2016; Li et al. 2018), and passage of the state data breach notification laws (Ashraf and Sunder 2023). Furthermore, Klein et al. (2022) conclude that passage of the GDPR more than doubled the discussion of cybersecurity risks in proxy statement filings. Calderon and Gao (2022) and Wang et al. (2022) report that SEC comment letters related to cybersecurity risks disclosure practices push registrants to increase the length and specificity of their cybersecurity risks disclosure as well as improve their readability.

[9] Studies may address multiple research questions and are classified in all relevant sections.

Other studies document that firms increase cybersecurity disclosure in response to public pressure, institutional pressure, and peer effects. While D'Arcy and Basoglu (2022) find that firms' cybersecurity disclosure practices are influenced by public pressure following a data breach, Jeyaraj and Zadeh (2020) report that institutional pressures have varying effects on firms' cybersecurity risks disclosure, providing evidence that such disclosure becomes isomorphic over time. Moreover, Barry et al. (2022) identified institutional setting as a discriminant factor of the difference between firms' cybersecurity disclosures.

However, results are mixed on influence of peer effects on firms' cybersecurity disclosure. While D'Arcy and Basoglu (2022) find that industry peer breaches prompt fewer cybersecurity disclosures in 8-K filings, Kelton and Pennington (2020) demonstrate experimentally that non-attacked firms' cybersecurity disclosure lessens the spillover effect of peer breaches on investors perception.

In the context of cybersecurity risk management disclosure, while Jeyaraj et al. (2020) and Jeyaraj and Zadeh (2021) report that the nature of cybersecurity threats influences firms' technical and non-technical response disclosure and impacts firms' transition between cybersecurity response actions over time, Nikkhah and Grover (2022) document that response disclosure of cyber incidents varies by the data breach notification laws' requirements.

Other studies focus on the characteristics of a cyber incident as disclosure drivers. Amir et al. (2018) find that severity of cyber incidents is a determinant of firms' underreporting cyberattacks. Similarly, but with respect to data breach notification disclosures, Jackson et al. (2019) document that managers obfuscate bad news associated with high data breach severity incidents by manipulating syntactical features of the data breach notification letters. Furthermore, others report that firms' prior breach experiences (Gao et al. 2020; Jiang et al. 2021) and breach-

related market reactions (Barry et al. 2022; Jiang et al. 2021) result in the provision of additional cybersecurity risks disclosure.

Researchers also identify various board governance determinants of cybersecurity disclosure. Nordlund (2019) finds that board expertise via interlock of cyber incidents increases the level and quality of cybersecurity risks disclosure in annual filings. Furthermore, Radu and Smaili (2020) report that board's gender composition influences the presence and level of cybersecurity disclosure. Moreover, there are other firms' characteristics that drive the content of cybersecurity disclosure including general levels of cybersecurity risks in business, company size, profitability, intangibility, industry, auditor change, and executive change (Gao et al. 2020).

Overall, studies on determinants of cybersecurity risks and incidents disclosure highlight the impact of regulatory pressure, public pressure, institutional pressure, threats, board governance and firm characteristics, peer effects, and characteristics of a cyber incident as drivers that influence disclosure of cybersecurity information.

### 2.4.2. Informativeness of cybersecurity disclosure

The cornerstone of cybersecurity disclosure is informing investors and other stakeholders. Prior reviews on the stock market reaction to disclosure of information security events arrive at conflicting conclusions, with Spanos and Angelis (2016) reporting a statistically significant reaction of security events on firms' stock price, whereas Richardson et al. (2019) document a small and short-lived stock market reaction to data breaches. Instead of focusing on informativeness of the disclosure of a specific cybersecurity event, this review focuses on the informativeness of *cybersecurity risks and incidents disclosure*. One can view informativeness at different levels of granularity, either the totality or sub-component of cybersecurity disclosure.

In totality, Gordon et al. (2010) find that information security voluntary disclosures are positively associated with the firm's market value. There is contradictory evidence of post SEC 2011 guidance cybersecurity risks disclosure on the stock market. While Morse et al. (2017) report that cybersecurity risks and incidents disclosing firms experience negative stock price effects to such disclosures, Berkman et al. (2018a) discover that the extent and relevance of such disclosure are valued higher by the market. Barry et al. (2022) emphasize that increased cybersecurity disclosures are associated with higher market valuation, and Obaydin et al. (2021) find that the enactment of data breach notification laws incentivizes managers to stockpile negative financial news leading to an increase in stock price crash risk.

Focusing on cybersecurity risks disclosure, Florakis et al. (2023) construct a firm-level measure of cybersecurity risk based on cybersecurity disclosures in annual reports and find that cybersecurity risk is priced as a systematic risk; consequently, investors demand a premium for holding stocks exposed to high cybersecurity risk. Similarly, but using quarterly earnings calls as a disclosure channel, Jamilov et al. (2021) confirm that high cyber risk stocks earn a higher return to compensate for the additional risk. Others report that disclosure of cybersecurity risk management activities, namely mitigation activities, are valued in the equity market (Bose and Leung 2019; Gordon et al. 2010), reduce the trading on private information (Berkman et al. 2018b), are less associated with cyber incidents, and experience less negative market reaction to a subsequent breach announcement (Wang et al. 2013).

Some studies examine the informativeness of cyber incidents disclosure. In contrast to Hilary et al. (2016), who failed to find a link between firms' cybersecurity disclosure and market reaction to subsequent breach announcements, others find that decrease in the level of cybersecurity disclosure after a breach is negatively related with market reaction (Chen et al. 2022)

and the use of social media disclosure channel exacerbates such impact (Rosati et al. 2019). Furthermore, studies show negative market reaction to firms' withholding disclosure of a cyber incident (Amir et al. 2018), to firms responding to an SEC cybersecurity comment letter (Wang et al. 2022), and to delayed disclosure of post cyber incident response (Gwebu et al. 2018; Nikkhah and Grover 2022).

Studies also document the impact of cybersecurity risks and incidents disclosure. Havakhor et al. (2020) find that disclosing cybersecurity investments are positively associated with performance measures and negatively associated with cost of capital. Others report that cybersecurity risks disclosure result in greater investment attractiveness when a firm had not disclosed a prior cyber incident (Frank et al. 2019) and when a firm discloses a cyber incident in a timely manner (Cheng and Walton 2019). Furthermore, research also indicates that not only do the content and language of cybersecurity risks disclosure influence companies' audit fees (Calderon and Gao 2021) but also the cyber incidents disclosure (Li et al. 2020).

The overall conclusions of studies on informativeness of cybersecurity risks and incidents disclosure are in line with the expectations of regulators in terms of usefulness of such disclosures to the equity market. Findings of these studies are consistent across the granularity levels of cybersecurity disclosure, whether the totality of disclosure or a sub-component thereof. Similar to the totality of disclosure, at the sub-component levels, the synthesis of studies' results highlights informativeness of disclosures of cybersecurity risks, risk management activities, and cyber incidents.

### 2.4.3 The content and quality of cybersecurity disclosure

The quality of cybersecurity risks and incidents disclosure depends on characteristics emphasized by the SEC guidance (2011 2018) of "a company-by-company approach [to

disclosure] that allows relevant and material information to be disseminated to investors without boilerplate language or static requirements while preserving completeness and comparability of information across companies […], avoid generic cybersecurity-related disclosure and provide specific information that is useful to investors." This review shows that cybersecurity risks and incidents disclosure are not in line with the SEC expectations in terms of content and quality.

Focusing on the context of SEC 2011 guidance, Li et al. (2018) document that presence and length of cybersecurity risks disclosure in the pre-guidance period are not boilerplate and associate with future cyber incidents; however, such association becomes insignificant post-guidance period. Similarly, but using peer data breaches, Ashraf (2021) reports lower quality of cybersecurity disclosure in post SEC guidance period, i.e., being more generic and less specific. Nonetheless, there is no agreement on the boilerplate nature of disclosures post SEC 2011 guidance (Berkman et al. 2018a).

In terms of content linguistic characteristics, cybersecurity disclosures in U.S. context are lengthier, less readable, more litigious, and disclosed mainly in Item 1A (Risk Factors) of 10-K filings, yet there are some instances where such disclosure are made in other sections of 10-K; namely, Items 1 (Business) and Item 7 (MD&A) (Gao et al. 2020). Furthermore, linguistic characteristics in terms of extent and relevance of cybersecurity disclosures are different between firms with different institutional settings such as foreign companies listed in U.S. exchanges (Barry et al. 2022). In the Canadian context, cybersecurity disclosure is relatively low, generic, vary widely in the amount of detail they provide, is disclosed in annual MD&A, and in some cases reiterated in annual information form and proxy statement (Héroux and Fortin 2020). Moreover, firms worldwide are discussing more cyber risk in conference calls, and such cyber-related

discussions are generally associated with more uncertainty and negative sentiment (Jamilov et al. 2021).

In the event of a cyber incident, results show that the attacked firms provide an insufficient amount of disclosure (Hilary et al. 2016) and disclose less about their own risk mitigation and business continuity and more about third-party risks (Cheong et al. 2021). Furthermore, while other studies show that cybersecurity disclosure expands after a severe incident and when a firm has prior cyber incident experience (Chen et al. 2022; Jiang et al. 2021; McGrath et al. 2022), Hilary et al. (2016) disagree and report no difference between breached and non-breached firms' disclosure.

Overall, results on the content and quality of cybersecurity risks and incidents disclosure indicate that quality of the cybersecurity disclosure falls short of the regulator intention. The synthesis of previous studies highlights that cybersecurity disclosure, contrary to what the SEC expects, is boilerplate, not unique, less readable, and more litigious. Furthermore, the analysis of the findings from the studies shows that the level of detail and completeness provided by companies in their disclosures regarding cyber incidents is limited.

### 2.4.4 Theory, methods, disclosure outlets, and incidents data sources

A prevalent trend observed in the current body of literature on cybersecurity risks and incidents disclosure is the lack of explicit theoretical underpinnings in the majority of the studies. Instead, authors tend to rely on inferences drawn from prior literature to justify their expectations. An examination of studies utilizing theoretical frameworks in the field of cybersecurity disclosure, as presented in Panel A of Table 2, reveals that several theories are recurrently employed, including, but not limited to, disclosure theory, voluntary disclosure theory, agency theory, legitimacy, signaling theory, and stakeholder theory. Furthermore, theories used come from a

diverse array of disciplines, including accounting, economics, finance, management, psychology, and sociology.

Panel B of Table 2 summarizes disclosure outlets used by studies on cybersecurity risks and incidents disclosure. The most used disclosure outlet, as expected, is annual reports (a total of 20 studies), followed by specific section of the annual reports (a total of 12 studies), and 8-k reports (a total of 4 studies). Additionally, it is noteworthy that the least utilized outlets for disclosure include conference calls and social media. However, while prior studies mainly examine cybersecurity disclosure in annual reports, considering other outlets such as conference calls, earnings press releases, media coverage and proxy statement might provide better understanding of how managers tailor their disclosure for different audiences (Kothari et al. 2009; Li 2010).

…….. [Insert Table 2 about here] ……...……...

Figure 2 presents a summary of the methodologies used by studies of cybersecurity risks and incident disclosure. Given the focal point of this review, which is disclosure, the most widely used methodology is textual and content analysis, as demonstrated by a total of 34 studies, followed by event studies, as reflected by a total of 19 studies, and experimental design, as illustrated by a total of 4 studies.[10] Only two studies employ a qualitative approach, namely case study.

In terms of cyber incidents disclosure, the most used data source is Privacy Rights Clearinghouse (PRC), followed by Audit Analytics cybersecurity database, and less frequently others, including Advisen, DatalossDB.org, Databreaches.net, ITRC/CyberScout Annual Data Breach Reports, Office of the Attorney General websites, and major media outlets, among others.

…….. [Insert Figure 2 about here] ……...……...

[10] Some studies use more than one methodology for example Berkman et al. (2018a).

## 2.5. Future directions

### 2.5.1 Determinants of cybersecurity disclosure

The current research examines limited governance characteristics such as board gender composition and board cybersecurity breach exposure, hence future research can explore other board governance characteristics and structures as drivers of cybersecurity disclosure practices. Furthermore, executive and management characteristics such as risk appetite, confidence level, power structure, reputation concerns, and compensation, among others, as well as organizational factors such as the presence of institutional investors, blockholders, access to funding, compliance and litigation risks all represent venues for future research. In addition, future studies can examine additional cyber risks composite scores and their association with level and/or content of cybersecurity disclosure.

### 2.5.2 Informativeness of cybersecurity disclosure

Although many studies examine the informativeness of cybersecurity risks and incidents disclosure to equity market, future research can explore disclosure beyond equity market including debt, cybersecurity, and cyber insurance markets. For example, given the idiosyncratic nature of cybersecurity risks, it is conceivable that the cyber insurance market will be more mature with a better level of cybersecurity disclosure. Future research can also examine the informativeness and/or impact of different cybersecurity risks and incidents disclosure at a more granular level. For example, is informativeness equally significant irrespective of the nature of cybersecurity risk management disclosure? Similarly, is disclosure of accepting cybersecurity risk valued the same as disclosure of cybersecurity risk transfer?

### 2.5.3 Content and quality of cybersecurity disclosure

Future studies can examine other qualitative characteristics of cybersecurity risks and incidents disclosure including, not only syntactic features but also semantic dimensions and how these vary across different disclosure outlets. Given that firms' have significant discretion in determining whether information regarding its cybersecurity is material enough to be disclosed to investors and if so what, where, when, and how much to disclose (Gordon et al. 2010), future research can tackle these questions with respect to both (1) disclosure of cybersecurity risks and countermeasures and (2) disclosure of cyber incidents and response measures. For example, a recent professional report reveals lack of consistency in the cyber incidents' disclosure outlets and even where exactly in a specific outlet (Audit Analytics 2022). Future research can expand on how the content and quality of cybersecurity disclosure vary across different disclosure outlets such as proxy statements, 8-k reports, and social media releases. Moreover, with respect to social media, a potential future venue is to explore the impact of public reaction on social media outlets in the form of sentiment analysis on cybersecurity incidents disclosure. The examination of the relationship between variations in cybersecurity risks and incidents disclosure and both firm-specific and country-specific characteristics is also a potential area of empirical inquiry. As the issue of cybersecurity continues to gain prominence, there has been a mounting interest among boards of directors, company executives, investors, regulators, and other stakeholders to gain insight into the measures that organizations are implementing to protect against, prepare for, and manage cybersecurity incidents. Thus, more research is needed exploring firms' disclosure of cybersecurity risk management.

## 2.6. Conclusion

This study provides an overview of the current state of cybersecurity risks and incidents disclosure as covered in the extant literature. The synthesis of previous studies' results suggests the presence of various factors that motivate companies to disclose information related to cybersecurity risks and incidents. The findings of these studies indicate that regulatory pressure, public pressure, institutional pressure, board governance and firm characteristics, peer effects, and characteristics of a cyber incident all have an impact on the disclosure of cybersecurity information. The extant literature on the topic of cybersecurity risks and incidents disclosure has revealed that, while the informativeness of such disclosures aligns with the expectations of regulators in terms of usefulness, the quality of such disclosures falls short of the regulatory expectations as indicated by the studies on the content and quality of cybersecurity risks and incidents disclosure.

The synthesis also has revealed the utilization of various theoretical frameworks, including, but not limited to, disclosure theory, voluntary disclosure theory, agency theory, and stakeholder theory. Additionally, the study observes, as expected, that annual reports, specific sections thereof, and 8-K reports are the most frequently studied outlets for disclosure in the field of cybersecurity risks and incidents, while conference calls and social media are the least commonly examined. Furthermore, the prevalent methodologies employed in studies on cybersecurity disclosure include textual and content analysis, event studies, and experimental design, with a limited application of qualitative methods.

This literature review contributes to research and practice by providing a comprehensive examination of the current state of research on cybersecurity risks and incidents disclosure. The study updates the existing literature by summarizing data sources, methodological approaches, and

theoretical perspectives while highlighting areas for future research. Furthermore, the review expands upon the work of prior literature that identified cybersecurity risks disclosure as a theme, by evaluating a broader and more recent set of literature as well as provides insights into the various components of such disclosure, including determinants, informativeness, content and quality, and theoretical frameworks. Moreover, the practical implications of the review are that firms should formulate a comprehensive disclosure policy to increase the transparency of cybersecurity risks and incidents reporting while minimizing their vulnerability and exposure. The limitations in the content and quality of cybersecurity disclosure call for improved compliance and regulatory monitoring.

This review is not without limitations. Firstly, a systematic approach is employed to select relevant literature for review, however, the scope of the reviewed studies was constrained by the search keywords and inclusion criteria utilized. Thus, it is possible that this review may have excluded studies that could contribute additional perspectives. Secondly, discussions of cybersecurity disclosure are prevalent in business reports and practitioner journals, which provide valuable practical insights; however, the present review only includes articles published in peer-reviewed academic journals or working papers.

## 2.7 References, figures, and tables

### References


Akey, P., Lewellen, S., Liskovich, I., & Schiller, C. (2021). Hacking corporate reputations. Working paper [SSRN3143740], Rotman School of Management.

American Institute of Certified Public Accountants (AICPA). (2017b). *SOC For Cybersecurity: Helping You Build Trust and Transparency.* Durham, NC: AICPA. available at: https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/soc-for-cybersecurity-brochure.pdf (accessed 10 March 2021)

American Institute of Certified Public Accountants (AICPA). (2017a). *AICPA Unveils Cybersecurity Risk Management Reporting Framework.* Available at: https://www.aicpa.org/press/pressreleases/2017/aicpa-unveils-cyber security-risk-management-reporting-framework.html (accessed 10 March 2021)

American Institute of Certified Public Accountants (AICPA). (2018). *Cybersecurity Risk Management Oversight: A Tool for Board Members*. Available at: https://www.thecaq.org/wpcontent/uploads/2019/03/caq_cyber security_risk_management_oversight_tool_2018-04.pdf (accessed 10 March 2021)

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

Ashraf, M. (2022). The role of peer events in corporate governance: Evidence from data breaches. *The Accounting Review*, *97*(2), 1-24.

Ashraf, M., & Sunder, J. (2023). Can shareholders benefit from consumer protection disclosure mandates? Evidence from data breach disclosure laws. *The Accounting Review*, *98*(4), 1-32.

Ashraf, M., (2021). Should the SEC allow managers discretion when disclosing risk factors? Evidence from peer data breaches and cyber risk factors. Working paper [ssrn3807487], DOI:10.2139/SSRN.3807487.

Audit Analytics. (2022). Trends in cybersecurity breach disclosures. Available at: https://www.auditanalytics.com/doc/AA_Trends_in_Cybersecurity_Report_April_2022 .pdf (Accessed July 6, 2022)

Barry, T., Jona, J., & Soderstrom, N. (2022). The impact of country institutional factors on firm disclosure: Cybersecurity disclosures in Chinese cross-listed firms. *Journal of Accounting and Public Policy*, *41*(6), 106998.

Berkman, H., Jona, J., Lee, G., & Soderstrom, N. (2018a). Cybersecurity awareness and market valuations. *Journal of Accounting and Public Policy*, *37*(6), 508-526.

Berkman, H., Jona, J., Lee, G., and Soderstrom, N. (2018b). Cybersecurity risk mitigation, private information leakage and earnings announcements. Working paper.

Beyer, A., Cohen, D. A., Lys, T. Z., & Walther, B. R. (2010). The financial reporting environment: Review of the recent literature. *Journal of Accounting and Economics*, 50(2-3), 296-343.

Bose, I., & Leung, A. C. M. (2019). Adoption of identity theft countermeasures and its short-and long-term impact on firm value. *MIS Quarterly*, 43(1), 313–327.

Calderon, T. G., & Gao, L. (2021). Cybersecurity risks disclosure and implied audit risks: Evidence from audit fees. *International Journal of Auditing*, *25*(1), 24-39.

Calderon, T. G., & Gao, L. (2022). Changes in corporate cybersecurity risk disclosures after SEC comment letters. *Journal of Accounting and Public Policy*, *41*(5), 106993.

Campbell, J. L., Chen, H., Dhaliwal, D. S., Lu, H. M., & Steele, L. B. (2014). The information content of mandatory risk factor disclosures in corporate filings. *Review of Accounting Studies*, *19*(1), 396–455.

Center for Audit Quality (CAQ). (2018). *CAQ Tool Helps Boards Oversee Cybersecurity Risk Management Of Public Companies* [Press Release]. Available at: https://www.thecaq.org/news/caq-tool-helps-boards-oversee-cybersecurity-riskmanagement-public-companies/ (Accessed April 7, 2021)

Chen, J., Henry, E., & Jiang, X. (2022). Is Cybersecurity Risk Factor Disclosure Informative? Evidence from Disclosures Following a Data Breach. *Journal of Business Ethics*, 1-26.

Cheng, X., & Walton, S. (2019). Do nonprofessional investors care about how and when data breaches are disclosed?. *Journal of Information Systems*, *33*(3), 163-182.

Cheong, A., Yoon, K., Cho, S., & No, W. G. (2021). Classifying the contents of cybersecurity risk disclosure through textual analysis and factor analysis. *Journal of Information Systems*, *35*(2), 179-194.

Coleman, D. (2018, April 11). *Nearly 65% of Affected Public Companies Did Not Report Cybersecurity Breaches to the SEC*. Audit Analytics. Available at: https://blog.auditanalytics.com/nearly-70-of-affected-public-companies-did-not-report-cybersecurity-breaches-to-the-sec/ (Accessed May 10, 2021)

Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2015). COSO in cyber age. Available at: https://www.coso.org/documents/COSO%20_in%20the_%20Cyber%20Age_FULL_r11.pdf (Accessed April 7, 2021)

Congressional Research Service. (2019). *Data protection law: An overview*. Available at: https://crsreports.congress.gov/product/pdf/R/R45631 (Accessed August 3, 2021)

Cram, W. A., D'arcy, J., & Proudfoot, J. G. (2019). Seeing the forest and the trees: A meta-analysis of the antecedents to information security policy compliance. *MIS Quarterly*, *43*(2), 525-554.

Crosignani, M., Macchiavelli, M., & Silva, A. F. (2023). Pirates without borders: The propagation of cyberattacks through firms' supply chains. *Journal of Financial Economics*, *147*(2), 432-448.

D'Arcy, J., & Basoglu, A. (2022). The influences of public and institutional pressure on firms' cybersecurity disclosures. *Journal of the Association for Information Systems*, *23*(3), 779-805.

Eaton, T. V., Grenier, J. H., & Layman, D. (2019). Accounting and cybersecurity risk management. *Current Issues in Auditing*, *13*(2), C1-C9.

Eisenbach, T. M., Kovner, A., & Lee, M. J. (2022). Cyber risk and the US financial system: A pre-mortem analysis. *Journal of Financial Economics, 145*(3), 802-826.

Ferraro, M. F. (2013). Groundbreaking or broken? an analysis of SEC cyber-security disclosure guidance, its effectiveness, and implications. *Albany Law Review*, 77(2), 297–346.

Florackis, C., Louca, C., Michaely, R., & Weber, M. (2023). Cybersecurity risk. *The Review of Financial Studies*, *36*(1), 351-407.

Frank, M. L., Grenier, J. H., & Pyzoha, J. S. (2019). How disclosing a prior cyberattack influences the efficacy of cybersecurity risk management reporting and independent assurance. *Journal of Information Systems*, *33*(3), 183-200.

Gansler, J. S., & Lucyshyn, W. (2005). Improving the security of financial management systems: What are we to do?. *Journal of Accounting and Public Policy*, *24*(1), 1-9.

Gao, L., Calderon, T. G., & Tang, F. (2020). Public companies' cybersecurity risk disclosures. *International Journal of Accounting Information Systems*, *38*, 100468.

Gordon, L. A., Loeb, M. P., & Sohail, T. (2010). Market value of voluntary disclosures concerning information security. *MIS Quarterly*, 567-594.

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & 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.

Gwebu, K. L., Wang, J., & Wang, L. (2018). The role of corporate reputation and crisis response strategies in data breach management. *Journal of Management Information Systems*, 35(2), 683-714.

Haapamäki, E., & Sihvonen, J. (2019). Cybersecurity in accounting research. *Managerial Auditing Journal, 34*(7), 808-834.

Havakhor, T., Rahman, M. S., & Zhang, T. (2020). Cybersecurity investments and the cost of capital. Working paper [SSRN 3553470].

He, C., HuangFu, J., Kohlbeck, M. J., & Wang, L. (2020). The impact of customer's reported cybersecurity breaches on key supplier's relationship-specific investments and relationship duration. Working paper [SSRN 3544245].

Héroux, S., & Fortin, A. (2020). Cybersecurity disclosure by the companies on the S&P/TSX 60 Index. *Accounting Perspectives*, *19*(2), 73-100.

Hilary, G., Segal, B., & Zhang, M. H. (2016). Cyber-risk disclosure: Who cares?. Working paper [2852519] Georgetown McDonough School of Business Research Paper.

Huang, H. H., & Wang, C. (2021). Do banks price firms' data breaches?. *The Accounting Review*, *96*(3), 261-286.

IBM. (2022). Cost of a data breach report 2022. Available at: https://www.ibm.com/security/data-breach (Accessed August 22, 2021)

Institute of Internal Auditors (IIA). (2016). *Assessing Cybersecurity Risk: Roles Of The Three Lines Of Defense.* Available at: https://na.theiia.org/standards-guidance/recommended-guidance/practice-guides/Pages/GTAG-Assessing-Cybersecurity-The-Three-Lines-Model.aspx (Accessed March 5, 2021)

Institute of Risk Management (IRM). (2014a). *Cyber Risk: Executive Summary.* Available at: https://www.theirm.org/media/8635/irm-cyber-risk-exec-summ-a5-low-res.pdf (Accessed March 5, 2021)

Institute of Risk Management (IRM). (2014b). *Cyber Risk Resources for Practitioners*. Available at: https://www.theirm.org/media/7237/irm-cyber-risk-resources-for-practitioners.pdf (Accessed March 5, 2021)

ISACA (2021). *COBIT Control Objectives for Information Technologies*. ISACA. Available at: https://www.isaca.org/resources/cobit (Accessed March 5, 2021)

ISO. (2013). *ISO/IEC 27002:2013 Information Technology- Security Techniques- Code of Practice for Information Security*. ISO. Available at: https://www.iso.org/standard/54533.html (Accessed March 5, 2021)

Jackson, S., Vanteeva, N., & Fearon, C. (2019). An investigation of the impact of data breach severity on the readability of mandatory data breach notification letters: Evidence from US firms. *Journal of the Association for Information Science and Technology*, *70*(11), 1277-1289.

Jamilov, R., Rey, H., & Tahoun, A. (2021). The anatomy of cyber risk. Working paper [No. w28906], National Bureau of Economic Research.

Janvrin, D. J., & Wang, T. (2022). Linking cybersecurity and accounting: An event, impact, response framework. *Accounting Horizons*, *36*(4), 67-112.

Jensen, M. C., & Meckling, W. H. (1976). Theory of the firm: Managerial behavior, agency costs and ownership structure. *Journal of Financial Economics*, *3*(4), 305-360.

Jeyaraj, A., & Zadeh, A. (2020). Institutional isomorphism in organizational cybersecurity: A text analytics approach. *Journal of Organizational Computing and Electronic Commerce*, *30*(4), 361-380.

Jeyaraj, A., & Zadeh, A. H. (2021). Exploration and exploitation in organizational cybersecurity. *Journal of Computer Information Systems*, DOI:10.1080/08874417.2021.1902424

Jeyaraj, A., Zadeh, A., & Sethi, V. (2020). Cybersecurity threats and organisational response: Textual analysis and panel regression. *Journal of Business Analytics*, *4*(1), 26-39.

Jiang W., Legoria, J., Reichelt, K., & Walton, S. (2021). Firm use of cybersecurity risk disclosure. *Journal of Information Systems*. *36*(1), 151-180.

Kamiya, S., Kang, J. K., Kim, J., Milidonis, A., & Stulz, R. M. (2021). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics*, *139*(3), 719-749.

Kappelman, L., Johnson, V. L., Maurer, C., Guerra, K., McLean, E., Torres, R., Snyder, M., & Kim, K. (2020). The 2019 SIM IT Issues and Trends Study. *MIS Quarterly Executive*, *19*(1).

Kelton, A. S., & Pennington, R. R. (2020). Do voluntary disclosures mitigate the cybersecurity breach contagion effect? *Journal of Information Systems*, *34*(3), 133-157.

Kitchenham, B., & Charters, S. (2007). Guidelines for performing systematic literature reviews in software engineering. Keele University, UK

Klein, A., Manini, R., & Shi, Y. (2022). Across the pond: How US firms' boards of directors adapted to the Passage of the General Data Protection Regulation. *Contemporary Accounting Research*, *39*(1), 199-233.

Kopp, E., Kaffenberger, L., & Wilson, C. (2017). Cyber risk, market failures, and financial stability. *International Monetary Fund*. https://ssrn.com/abstract=3024075

Li, F. (2010). Textual analysis of corporate disclosures: A survey of the literature. *Journal of Accounting Literature*, *29*(1), 143-165.

Li, H., No, W. G., & Boritz, J. E. (2020). Are external auditors concerned about cyber incidents? Evidence from audit fees. *Auditing: A Journal of Practice & Theory*, *39*(1), 151-171.

Li, H., No, W. G., & Wang, T. (2018). SEC's cybersecurity disclosure guidance and disclosed cybersecurity risk factors. *International Journal of Accounting Information Systems*, *30*, 40-55.

Loughran, T., & McDonald, B. (2016). Textual analysis in accounting and finance: A survey. *Journal of Accounting Research*, *54*(4), 1187-1230.

Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data privacy: Effects on customer and firm performance. *Journal of Marketing*, *81*(1), 36-58.

Massaro, M., Dumay, J., & Guthrie, J. (2016). On the shoulders of giants: Undertaking a structured literature review in accounting. *Accounting, Auditing & Accountability Journal*, *29*(5), 767–801.

McGrath, V., Sheedy, E. A., & Yu, F. (2022). Governance of cyber security: State of play. Working paper [SSRN3971177], http://dx.doi.org/10.2139/ssrn.3971177.

Morse, E. A., Raval, V., & Wingender Jr, J. R. (2017). SEC cybersecurity guidelines: Insights into the utility of risk factor disclosures for investors. *The Business Lawyer*, *73*(1), 1-34.

National Conference of State Legislatures. (2020). *Security Breach Notification Laws*. NCSL. Available at: https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx (accessed January 6, 2022)

National Initiative for Cybersecurity Careers and Studies (NICCS). (2022). A glossary of common cybersecurity words and phrases. Available at: https://niccs.cisa.gov/cybersecurity-career-resources/glossary#C (Accessed December 2, 2022)

National Institute of Standards and Technology (NIST). (2018). *Framework For Improving Critical Infrastructure Cybersecurity, Version 1.1.* NIST. Available at: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.041 62018.pdf (Accessed March 5, 2021)

Nikkhah, H. R., & Grover, V. (2022). An empirical investigation of company response to data breaches. *MIS Quarterly*, *46*(4), 2163-2196.

Nordlund, J. (2019). The disclosure of cybersecurity risk. Working paper [SSRN 3926962].

Obaydin, I., Xu, L., & Zurbruegg, R. (2021). The unintended cost of data breach notification laws: Evidence from managerial bad news hoarding. working paper [SSRN 3926962].

Public Company Accounting Oversight Board (PCAOB). (2018). *Standing Advisory Group Meeting Panel Discussion – Cybersecurity*. PCAOB. Available at: https://pcaobus.org/News/Events/Documents/Cybersecurity%20Briefing%20Paper.pdf (Accessed April 7, 2021)

Radu, C., & Smaili, N. (2022). Board gender diversity and corporate response to cyber risk: Evidence from cybersecurity related disclosure. *Journal of Business Ethics*, *177*(2), 351-374.

Rosati, P., Deeney, P., Cummins, M., Van der Werff, L., & Lynn, T. (2019). Social media and stock price reaction to data breach announcements: Evidence from US listed companies. *Research in International Business and Finance*, 47, 458-469.

Rubin, G. T. (2019, February 26). *Many Company Hacks Go Undisclosed to SEC Despite Regulator Efforts*. *Wall Street Journal*. Available at: https://www.wsj.com/articles/many-company-hacks-go-undisclosed-to-sec-despite-regulator-efforts-11551218919 (Accessed October 24, 2021)

Securities and Exchange Commission (SEC). (2005). Securities and Exchange Commission final rule, release no.33–8591(fr-75). Available at: http://www.sec.gov/rules/final/33-8591.pdf. (Accessed February 2, 2021)

Securities and Exchange Commission (SEC). (2011). Cf disclosure guidance: Topic no. 2. Available at: Https://www.Sec.Gov/divisions/corpfin/guidance/cfguidance-topic2.Htm. (Accessed February 2, 2021)

Securities and Exchange Commission (SEC). (2018). Commission statement and guidance on public company cybersecurity disclosures. Release Nos. 33-10459; 34-82746. Available at: https://www.sec.gov/rules/interp/2018/33-10459.pdf (Accessed February 2, 2021)

Securities and Exchange Commission (SEC). (2020a). Modernization of regulation S-K items 101, 103, and 105 - final rule, release nos. 33-10825; 34-89670; file no. S7-11-19; RIN 3235-AL78. Available at: https://www.sec.gov/rules/final/2020/33-10825.pdf (Accessed March 3, 2022)

Securities and Exchange Commission (SEC). (2020b). Press release - SEC adopts rule amendments to modernize disclosures of business, legal proceedings, and risk factors under Regulation S-K. Available at: https://www.sec.gov/news/press-release/2020-192 (Accessed March 3, 2022)

Securities and Exchange Commission (SEC). (2022). Proposed rule: Cybersecurity risk management, strategy, governance, and incident disclosure. Available at: https://www.sec.gov/rules/proposed/2022/33-11038.pdf. (accessed March 14, 2022)

Skinner, D. J. (1994). Why firms voluntarily disclose bad news. *Journal of Accounting Research*, *32*(1), 38-60.

Smedinghoff, T. J. (2015). An overview of data security legal requirements for all business sectors. Working paper [SSRN 2671323], http://dx.doi.org/10.2139/ssrn.2671323

Spanos, G., & Angelis, L. (2016). The impact of information security events to the stock market: A systematic literature review. *Computers & Security*, *58*, 216-229.

Spence, M. (1973). Job market signaling. *The Quarterly Journal of Economics*, *87*(3), 355–374.

Steinbart, P. J., Raschke, R. L., Gal, G., & 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.

Steinbart, P. J., Raschke, R. L., Gal, G., & Dilla, W. N. (2018). The influence of a good relationship between the internal audit and information security functions on information security outcomes. *Accounting, Organizations and Society*, *71*, 15-29.

Sumner, P., Day J., & Mahoney, M. (2020). Cybersecurity: An evolving governance challenge *Harvard Law School Forum on Corporate Governance.* Available at: https://corpgov.law.harvard.edu/2020/03/15/cybersecurity-an-evolving-governance-challenge/ (Accessed May 17, 2021)

Verizon Enterprise Solutions. (2015). Verizon 2015 data breach investigations report. *Verizon Enterprise Solutions*. Available at: http://www.verizonenterprise.com (Accessed May 20, 2021).

Verrecchia, R. E. (1983). Discretionary disclosure. *Journal of Accounting and Economics*, *5*, 179-194.

Walton, S., Wheeler, P. R., Zhang, Y. I., & Zhao, X. R. (2020). An integrative review and analysis of cybersecurity research: Current state and future directions. *Journal of Information Systems*, *35*(1), 155–186.

Wang, T., Kannan, K. N., & Ulmer, J. R. (2013). The association between the disclosure and the realization of information security risk factors. *Information Systems Research*, *24*(2), 201-218.

Wang, T., Yen, J. C., & Yoon, K. (2022). Responses to SEC comment letters on cybersecurity disclosures: An exploratory study. *International Journal of Accounting Information Systems*, *46*, 100567.

World Economic Forum. (2020). Global risks report 2020. Available at: https://www.weforum.org/reports/the-global-risks-report-2020/ (Accessed May 20, 2021).

**FIGURE 1 The Process to Find the Final Number of Papers**

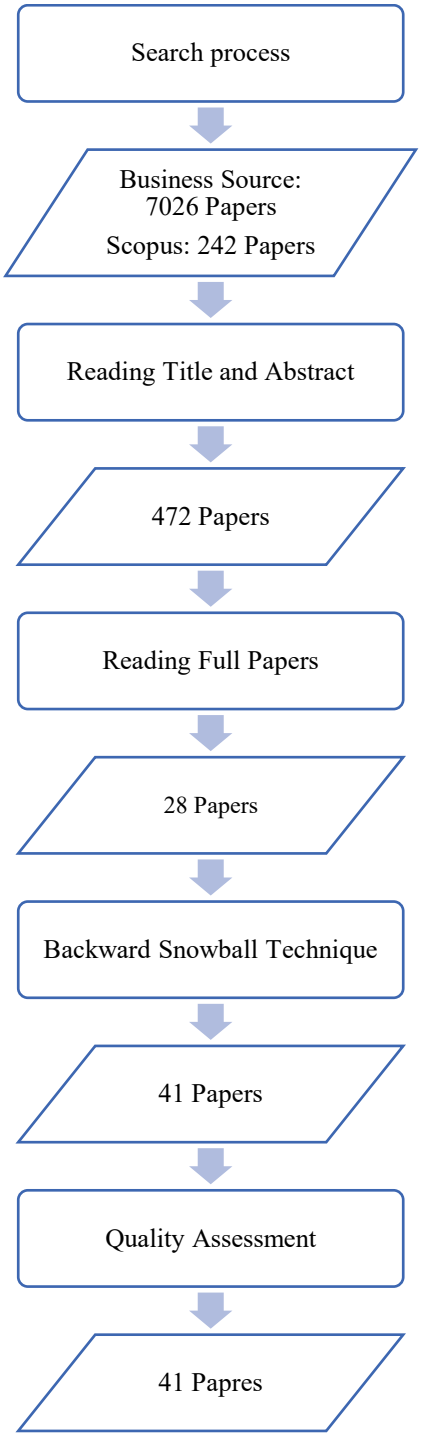

**FIGURE 2 Methods Used Across the Cybersecurity Risks and Incidents Disclosure Literature**

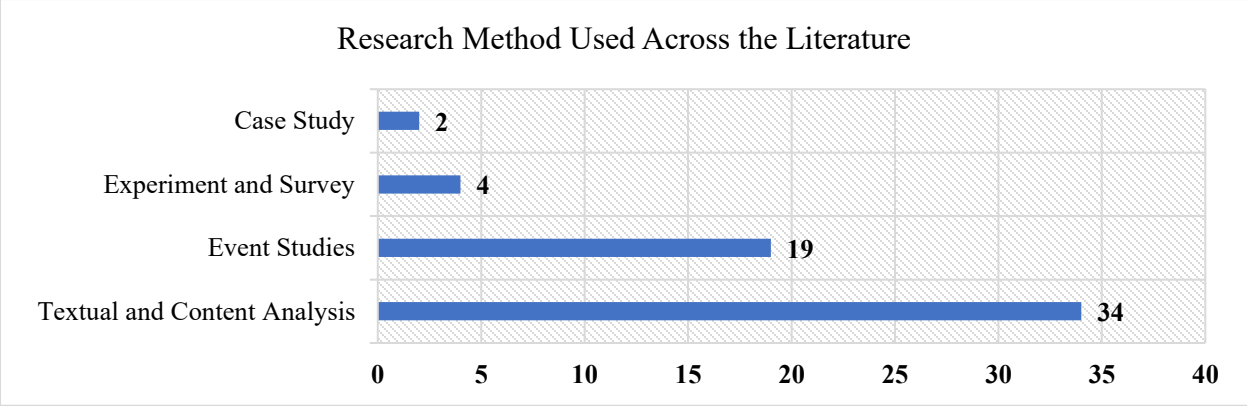

**TABLE 1 Summary of Cybersecurity Disclosure Studies**

| **Determinants of Cybersecurity Risks and Incidents Disclosure** | | | |
|---|---|---|---|
| **Author(s)** | **Journal Title** | **Research Objective** | **Findings** |
| Amir et al. (2018) [I] | Review of Accounting Studies | Investigate the extent to which firms withhold information on cyberattacks. | Managers tend to disclose less severe attacks and withhold information on attacks that cause greater damage from investors. |
| Ashraf and Sunder (2023) | The Accounting Review | Examine impact of data breach notification laws on shareholder risks. | Data breach notification laws reduce shareholder risk by incentivizing managers to take real actions to reduce firms' exposure to cyber risk and the likelihood of experiencing a data breach. |
| Barry et al. (2022) [C, I] | Journal of Accounting and Public Policy | Examine differences in qualitative disclosures (i.e., cybersecurity awareness) between Chinese firms that cross listed in the U.S. and their U.S. domestic counterparts. | Chinese cross-listed firms in the U.S. provide less cybersecurity disclosure related to cybersecurity awareness than their U.S. domestic counterparts. |
| Calderon and Gao (2022) | Journal of Accounting and Public Policy | Explore the cybersecurity risk disclosure' comment letter and the following cybersecurity risk disclosures changes. | Firms increase (decrease) the length, readability, and specificity (uncertainty) of cybersecurity risk disclosures after receiving a comment letter. |
| D'Arcy and Basoglu (2022) | Journal of the Association for Information Systems | Investigate impact of public and institutional pressures on timeliness of cybersecurity disclosure. | While public pressure prompt more cybersecurity disclosure, industry peer breaches prompt fewer cybersecurity disclosures in 8-K filing. |

| Author(s) | Journal Title | Research Objective | Findings |
|---|---|---|---|
| Gao et al. (2020) [C] | International Journal of Accounting Information Systems | Study the content and linguistic characteristics of firms' cybersecurity risk disclosure practices as well as factors that drive disclosure trends. | Cybersecurity risks disclosure become lengthier, less readable, more litigious, disclosed in Item 1A Risk Factors and the most frequently disclosed cybersecurity issues are risks related to service and operation disruption and losing confidential data. |
| Gordon et al. (2006) | Journal of Accounting and Public Policy | Examine impact of the Sarbanes-Oxley Act on the corporate disclosures of information-security activities | Passage of SOX has a positive impact on a firm's voluntary disclosure of corporate information-security activities. |
| Hilary et al. (2016) [C, I] | Working Paper | Investigate whether lack of cybersecurity disclosure is justifiable or rather reflects a market failure. | Cybersecurity disclosures are scarce, generic, and show no difference between breached and non-breached firms. |
| Jackson et al. (2019) | Journal of the Association for Information Science and Technology | Explore the impact of data breach severity on syntactical features of data breach notification letters. | Managers obfuscate bad news associated with severe data breach incidents by manipulating syntactical features of the data breach notification letters. |
| Jeyaraj and Zadeh (2020) | Journal of Organizational Computing and Electronic Commerce | Examine how organizational cybersecurity responses disclosure become isomorphic over time. | Mimetic pressures are significant over time while coercive pressures are significant in the near-term and normative pressures are significant in the long-term. |
| Jeyaraj and Zadeh (2021) | Journal of Computer Information Systems | Examine the firms' exploration and exploitation cybersecurity responses to cybersecurity threats. | Firms alternate between exploration and exploitation cybersecurity responses over time. |

| Author(s) | Journal Title | Research Objective | Findings |
|---|---|---|---|
| Jeyaraj et al. (2020) | Journal of Business Analytics | Explore the relationship between cybersecurity threats and firms' cybersecurity responses (technical and non-technical) disclosure. | Cybersecurity threats impact firms' technical and non-technical cybersecurity responses disclosure. |
| Jiang et al. (2021) [C] | Journal of Information Systems | Explore firms' cybersecurity disclosures following a data breach incident. | Provision of additional cybersecurity risk disclosures following a data breach is contingent on the firm's prior breach experience and its related market reaction. |
| Kelton and Pennington (2020) | Journal of Information Systems | Examine whether voluntary cybersecurity disclosures alleviate investors' negative perceptions of a non-breached firm following a breach at an industry peer firm. | Provision of cybersecurity disclosures both prior to and after a breach announcement at an industry peer firm, can mitigate the contagion effect for investors. |
| Klein et al. (2022) | Contemporary Accounting Research | Investigate the change in boards' cybersecurity risk oversight following the implementation of GDPR. | Passage of the GDPR more than doubled the discussion of cybersecurity risks in proxy statements. |
| Li et al. (2018) | International Journal of Accounting Information Systems | Examine association between the presence and length of cybersecurity risks disclosure and likelihood of subsequent cyber incidents both before and after the SEC's 2011 guidance. | The presence and the length of cybersecurity risks disclosure prior to the SEC's guidance are related to future cyber incidents and such association becomes insignificant post SEC 2011 guidance. |
| Nikkhah and Grover (2022) [I] | MIS Quarterly | Investigate the effect of breached firms' cybersecurity incident response strategies and | Companies can positively influence customer and investor behavior through accommodative response strategies such as apologies or compensation, rather |

| Author(s) | Journal Title | Research Objective | Findings |
|---|---|---|---|
| | | response timeliness on customers and investors. | than corrective actions; and timeliness of the response enhances the effectiveness of such strategies. |
| Nordlund (2019) | Working Paper | Examine the effect of directors' cyber incident exposure via interlock on focal firm cybersecurity risk disclosure. | Focal firms' disclosure level and quality of cybersecurity risk improves with director experience of a cyber incident at an interlocking firm. |
| Radu and Smaili (2020) | Journal of Business Ethics | Investigate effect of board's gender composition on the extent of cybersecurity disclosure. | Positive association between the presence and level of cybersecurity disclosure and board gender diversity (with at least three women). |
| Wang et al. (2022) | International Journal of Accounting Information Systems | Study firms' cybersecurity disclosures change following cybersecurity risk disclosures' comment letters and the market reaction to the firms' response letter. | Comment letter firms revised their cybersecurity disclosures, and their response letters are associated with negative market reaction. |
| **Informativeness of Cybersecurity Risks and Incidents Disclosure** | | | |
| **Author(s)** | **Journal Title** | **Research Objective** | **Findings** |
| Berkman et al. (2018a) [C] | Journal of Accounting and Public Policy | Examine the association between the cybersecurity awareness score and market value. | Positive association between firms' cybersecurity awareness and market value. |
| Berkman et al. (2018b) | Working Paper | Investigate the impact of cybersecurity risk management measures disclosure on the trading and pricing of private information prior to earnings information. | Firms with more extensive cybersecurity risk mitigation in their annual reports experience significant price changes at the announcement. |

| Author(s) | Journal Title | Research Objective | Findings |
|---|---|---|---|
| Morse et al. (2017) | The Business Lawyer | Examine companies' cybersecurity disclosures post SEC 2011 guidance. | Cybersecurity risks disclosing firms generally experienced significant negative stock market price effects. |
| Wang et al. (2013) | Information Systems Research | Assess the association between the nature of information security disclosures and future media announcements of breaches. | Disclosing cybersecurity risk-mitigation themes is less likely to be followed by future breaches and market reactions to announcements of breaches differ based on prior disclosure. |
| Gordon et al. (2010) | MIS Quarterly | Assess market value of voluntary disclosures of items pertaining to information security. | Voluntarily information security discloser is positively associated with the market value of a firm. |
| Jamilov et al. (2021) [C] | Working Paper | Develop a text-based measures of firm-level cyber risk exposure and predict future cyberattacks. | Firms have positive exposure to cyber risk based on earnings call are significantly more likely to report a cyberattack within the next 8 quarters. |
| Gwebu et al. (2018) | Journal of Management Information Systems | Explore the relative efficacy of firm reputation and a range of post-breach response strategies and market reaction. | Lower reputation firms suffer negative returns after a breach disclosure and effectiveness of their response strategies in mitigating the negative impact on their value remains questionable. |
| Chen et al. (2022) [C] | Journal of Business Ethics | Investigate the changes in cybersecurity risks disclosure following a data breach and the market reaction to such changes. | Firms tend to increase the cybersecurity disclosures following a breach incident, particularly when the breach is severe. |
| Florakis et al. (2023) | The Review of Financial Studies | Construct a firm-level measure of cybersecurity risk and examine whether it is priced in | Cybersecurity risk is priced as a systematic risk factor and investors require a premium to hold stocks exposed to high cybersecurity risk. |

| Author(s) | Journal Title | Research Objective | Findings |
|---|---|---|---|
| | | the cross section of stock returns. | |
| Obaydin et al. (2021) | Working Paper | Investigate impact of state-level data breach notification laws on firm's bad news hoarding. | Enactment of data breach notification laws incentives managers to stockpile negative financial news leading to an increase in stock price crash risk. |
| Bose and Leung (2019) | MIS Quarterly | Analyze the short- and long-term impact of adoption of countermeasures of cyber identity theft on the firms' market value. | Disclosure of cyber identity theft countermeasures' adoption is rewarded in the equity market. |
| Rosati et al. (2019) | Research in International Business and Finance | Investigate the effect of social media usage as alternative communication channel by breached firms on stock price reaction to a breach announcement. | Communication via social media exacerbate the negative impact of breach announcements on stock price particularly when firms announce the breach via social media. |
| Calderon and Gao (2021) **IM** | International Journal of Auditing | Explore the association between firms' cybersecurity risk disclosures and audit fees. | Audit fees are influenced by the cybersecurity risk disclosures' content (number of words) and language (readability and litigious language). |
| Havakhor et al. (2020) **IM** | Working Paper | Examine the value-creation path of cybersecurity investments disclosure in SEC filings. | Disclosure of cybersecurity investments are associated with a reduction in cost of capital and robust positive value of book-keeping measures of performance. |
| Li et al. (2020) **IM** | Auditing: A Journal of Practice & Theory | Investigate whether external auditors adjust their audit fees based on concern for cybersecurity risks and | Severe cyber incidents are associated with increases in audit fees and the increase is smaller for firms with prior cybersecurity risk disclosure post 2011 SEC guidance. |

| Author(s) | Journal Title | Research Objective | Findings |
|---|---|---|---|
| | | incidents disclosure before and after incidents. | |
| Frank et al. (2019) IM | Journal of Information Systems | Investigate the relationship between prior cyberattack disclosure and the efficacy of the management and insurance components of the AICPA's cybersecurity reporting framework. | The AICPA's cybersecurity reporting framework's management component is more effective without assurance when a company has not disclosed a prior cyberattack, but obtaining third-party assurance is more beneficial for companies that have disclosed one. |
| Cheng and Walton (2019) IM | Journal of Information Systems | Investigate the influence of cybersecurity disclosure's timing and source on nonprofessional investors' perceptions of a company experiencing a data breach. | Investors exhibit the least favorable evaluations towards companies that originate disclosures that are not timely, while timely disclosure leads to investors committing more capital. |

**Content and Quality of Cybersecurity Risks and Incidents Disclosure**

| Author(s) | Journal Title | Research Objective | Findings |
|---|---|---|---|
| McGrath et al. (2022) | Working Paper | Assess the current state in cybersecurity governance. | Cybersecurity disclosure expands following a severe cyberattack. |
| Cheong et al. (2021) | Journal of Information Systems | Explore how a firm's cybersecurity risks disclosure behaviors differ when it experienced a cyber incident or received an adverse SOX 404 opinion. | Breached firms provide insufficient amount of disclosure about their incident control and risk mitigation and business continuity but disclose more about the third-party risks. |

| Author(s) | Journal Title | Research Objective | Findings |
|---|---|---|---|
| Héroux and Fortin (2020) | Accounting Perspectives | Examine whether the content of cybersecurity disclosures of Canadian firms comprising the S&P/TSX 60 index is aligned with financial regulators' guidelines. | Canadian firms exhibit a limited level of cybersecurity disclosure, detail, and specificity, and are primarily disclosed in their annual MD&A. |
| Ashraf (2021) | Working Paper | Examine the effect of peer data breaches on the uniqueness of cyber risk factors disclosure both before and after the SEC's 2011 guidance. | The SEC's 2011 guidance constrained managerial discretion and resulted in lower quality (i.e., less unique) of cyber risk factor disclosures. |

[C] Content and Quality, [I] Informativeness, [IM] Impact

**TABLE 2 Theories and Disclosure Outlets**

| **Panel A: Theory Used** | | | |
|---|---|---|---|
| | Determinants | Informativeness | Content and Quality |
| Agency theory | * | * | * |
| Attribution theory | | * | |
| Auditing theory | | * | |
| Cognitive dissonance theory | | * | |
| Cost-benefit analyses theory | * | | |
| Crisis management theory | | * | |
| Critical mass theory | * | | |
| Cue utilization theory | | * | |
| Disclosure theory | * | * | * |
| Efficient market theory | | * | |
| Expectancy violation theory | * | | |
| Institutional theory | * | * | |
| Instrumental stakeholder theory | * | | * |
| Legitimacy theory | * | | |
| Liability theory | | * | |
| Resource dependence theory | * | | |
| Signaling theory | * | | |
| Spreading activation theory | | * | |
| Stakeholder theory | * | * | * |
| Voluntary disclosure theory | * | * | * |

| **Panel B: Disclosure Outlet Examined** | | | | |
|---|---|---|---|---|
| | Determinants | Informativeness | Content and Quality | Total |
| Annual reports | 8 | 8 | 7 | 23 |
| Section of annual reports | 7 | 4 | 5 | 16 |
| Quarterly reports | | 2 | 1 | 3 |
| 8-K reports | 1 | 2 | 1 | 4 |
| Comment letters | 2 | 1 | | 3 |
| Conference call | | 1 | 1 | 2 |
| Data breach notification letters | 2 | 2 | | 4 |
| News release | | 1 | 1 | 2 |
| Proxy statements | 1 | | 2 | 3 |
| Social media | | 1 | | 1 |

## Chapter 3: Who Has Oversight Responsibility for Cybersecurity Risk and Does It Matter?


### Abstract

The omnipresence of cybersecurity risk is well-documented, yet its board-level oversight received little attention. This study examines where cybersecurity risk oversight resides within a firm's governance structure, what determines such positioning, and how it impacts the firm's response to a cybersecurity breach. In proxy statements for breached firms, only a minority of firms explicitly disclose their cybersecurity risk oversight with a wide variation in such assignment, ranging from the full board to a named board committee(s) - the audit committee being the most common choice. Furthermore, results show that board connectedness and cyber competency are positively associated with firms disclosing assignment of oversight, the full board oversight is more likely with smaller boards, and boards' shareholding and cybersecurity experience steer oversight assignment to the audit committee. In the event of a breach, the presence of oversight decreases the time firms take to announce and resolve such a breach as well as the recurrence of breaches. Moreover, while audit committee oversight is more effective in timeliness of breach disclosure and resolution, full board oversight is more effective in reducing breach recurrence. These results suggest that oversight should be viewed as a core governance tool in preventing and mitigating cybersecurity risks.



**Keywords:** Cybersecurity, risk oversight, corporate governance, data breaches, determinants, consequences


### 3.1 Introduction

Cybersecurity breaches continue to accelerate in frequency, severity, and impact. In 2022, average data breach costs were at their highest in the last 17 years, rising from USD 4.24 million in 2021 to USD 4.35 million in 2022 (IBM 2022). Organizations currently allocate more than USD

150 billion annually towards cybersecurity, a figure that is expected to exceed USD 200 billion by 2025 (Gartner 2021). A successful cyber-attack can cause an organization's loss of value and reputation, increase its cost of capital, lead to regulatory scrutiny and/or litigation, and compromise corporate intellectual property and clients' data (Frank et al. 2021; Huang and Wang 2021; Banker and Feng 2019; Yen et al. 2018). Thus, cybersecurity breaches are an omnipresent risk to firms and, therefore, require board oversight. The Securities Exchange Commission (SEC) stipulates that overall risk oversight is the responsibility of the board (SEC 2009). However, there is no specific due care standard or regulator guidance for boards to assign the responsibility of cybersecurity risk oversight (Loop 2016), resulting in substantial variation in practice (Klemash et al. 2020). Hence, the objective of this study is three-fold. First, the study examines who has governance responsibility to oversee cybersecurity risk. Second, the study seeks to identify the key governance determinants of cybersecurity risk oversight, analyzing how these determinants may vary across different oversight setups. Third, to explore the effectiveness of firms' cybersecurity risk oversight, the study examines the relationship between a firm's oversight setup and its response to cybersecurity breaches.

The study focuses on board cybersecurity risk oversight for several reasons. First, board oversight sets the tone at the top, thus influencing organizational cybersecurity culture, providing legitimacy for risk management, and steering employee compliance and sense of accountability towards cybersecurity risk practices (Beasley et al. 2022; Braumann et al. 2020; Maurer et al. 2021). Second, the governance implications for the cybersecurity risks are not yet fully understood (Rajgopal and Srinivasan 2016) and received notably less attention from academic literature than the technical aspects of cybersecurity (Slapničar et al. 2022), as well as that there is a need for proactively managing cybersecurity risks (Sonnemaker 2019). Finally, investor groups demand

that boards be active and explicit about cybersecurity risk oversight and management (Davis 2016) as a large portion of the costs of breaches is borne by them (Clayton 2017).

The increase in the number of publicized cyber-attacks led the SEC to issue cybersecurity disclosure guidance in 2011 and 2018 to assist publicly traded companies in preparing and reporting their cybersecurity disclosures to investors (SEC 2011; 2018). Currently, the SEC is reviewing a new proposed rule, which seeks to improve public companies' disclosures of cybersecurity risk management, strategy, governance, and incident reporting (SEC 2022). More relevant to this study, the new rule in part intends to require public companies to make periodic disclosures about board of directors' oversight of cybersecurity risk. In addition, all 50 U.S. states have enacted regulations to help mitigate the impact of cybersecurity breaches. Furthermore, many professional bodies issued cybersecurity-related policies, procedures, guidelines, and frameworks. Despite these regulations and guidelines, the SEC did not take a position on the assignment of cybersecurity risk oversight responsibility (Loop 2016) and allowed each entity to determine to whom it assigns such responsibility. Under such discretion cybersecurity risk oversight still struggles to find a home in the boardroom (PwC 2018).

On the one hand, there is an efficiency-based view that the full board should oversee cybersecurity risk and not delegate to a committee or subcommittee (Rothrock et al. 2018), for cost considerations or to avoid the perception that the board lacks appropriate expertise (Higgs et al. 2016; Jewer and McKay 2012). On the other hand, reflecting a competency-based view, there are factors that constrain the full board involvement in the oversight of cybersecurity risk, leading the board to delegate it to a board-level committee (Price and Lankton 2018; Higgs et al. 2016). These factors include the board's low IT knowledge and experience (Turel and Bart 2014), a failure to attribute sufficient strategic importance to IT within the organization (Nolan and McFarlan

2005), and the potential that a board-level committee is more suitable for close and enhanced monitoring and evaluation of cyber risks and issues.

Using a combination of textual analysis of firms' proxy statements (DEF 14A), with manual extraction of oversight assignment, and breach events from Advisen Ltd. (Cyber Loss Data) during 2010-2020, this study addresses the question of whether boards oversee cybersecurity risk directly or assign it to a board-level committee.[11] The analysis reveals that most firms do not disclose the board's role in cybersecurity risk oversight in their proxy statements. Firms started to increasingly disclose oversight assignment shortly after the SEC 2011 cybersecurity guidance. Of those that explicitly assign oversight responsibility, 84 percent disclose that it is assigned to a board-level committee(s) and 16 percent to the full board. Exploratory analysis shows variation in board-level committee(s) assignment across industry sectors, including committees for audit, finance, technology, compliance, risk, cybersecurity, nominating and governance, to a joint committee, or other. However, most firms assign oversight to the audit committee, risk committee, or technology committee. The analysis also reveals that five percent of firms shift the cybersecurity risk oversight responsibility from one board or board committee(s) to another. Overall, these findings align with the regulator's decision of leaving the choice of oversight assignment to the board of directors, possibly to accommodate the varying particularities of firms and industry sectors.

[11] The Advisen Cyber Loss Data is a proprietary dataset that covers cybersecurity incidents around the world. It collects information from reliable and publicly verifiable sources such as SEC filings, press releases, business press, websites, newspaper articles, newsfeeds, specialized legal information services, court rulings, multiple online data breach clearinghouses and federal and state governments in the United States. This dataset is more comprehensive than the publicly available and widely used Privacy Rights Clearinghouse. It provides detailed information of cyber events, including case type, case status, event disclosure date, information being compromised, breached date, number of records being affected, actors, source of loss, type of loss, and amount of loss, among others. Previous studies have used this dataset such as Aldasoro et al. (2022), Chande and Yanchus (2019), and Romanosky (2016). For more information: https://www.advisenltd.com/about/

Prior research does not systematically address the determinants or the consequences of the governance of cybersecurity risk oversight. Thus, building on the insights gained from the analysis of cybersecurity risk governance responsibility in the first objective, the study now turns to examining the governance determinants of cybersecurity risk oversight using a cascading three-level analysis approach. To achieve that, and for simplicity, the study categorizes ten variations of cybersecurity risk oversight responsibility into three groups: full board, audit committee, and non-audit board-level committee(s).

At the first level, the study examines the governance determinants of assigning cybersecurity risk oversight responsibility. The results suggest that the board's cyber competency, network size, equity holding, and gender diversity are significant determinants of whether firms explicitly assign cybersecurity risk oversight responsibility or not. The findings reveal that while the board's cyber experience and network size positively contribute to the assignment, equity ownership and gender diversity exhibit a negative impact. In addition to these factors, the study highlights the significant role of organizational factors in determining oversight responsibility assignment. These factors include the presence of cybersecurity role and risk management framework at the management level. This finding corroborates Lowry et al.'s (2021) conclusion that directors rely heavily on chief information security officers to "coach" them on cybersecurity oversight. Nonetheless, the findings indicate that the presence and interaction of risk, compliance, and technology committees with financial/non-financial sectors has a negative impact on explicit cybersecurity risk oversight responsibility assignment.

At the second level, examining the governance determinants of assigning oversight responsibility to the full board or to a board-level committee(s), the study finds that full boards oversee cybersecurity risk in firms with smaller boards. This finding supports the notion that the

bigger the board size, the more likely the assignment of oversight is to a board-level committee(s) for closer oversight and monitoring of cyber risks and issues, and that larger boards may be better equipped to establish specialized board-level committee to oversee such risks.

At the third level, looking at governance determinants of assigning oversight to the audit committee or a non-audit board-level committee(s), the results indicate that while boards with more equity ownership and cyber experience are more likely to delegate oversight to the audit committee, larger boards with bigger network size are more likely to assign it to a non-audit committee(s). This finding aligns with prior research that documents the positive impact of technology experience in general on the effectiveness of committee performance (Ashraf et al. 2020b; Hadden et al. 2003) and therefore steering the board to assign oversight to the audit committee possibly because of its experience with risk oversight and compliance and efficiency of such assignment. Moreover, board's equity ownership leads to better alignment of the board's interest with that of shareholders, and make boards pursue decisions that protect such wealth, incentivizing them to assign oversight to the audit committee as it is perceived to be more experienced with risk activities. Moreover, in supplementary analysis, the study reveals that in organizations where risk, compliance, and/or technology committees exist, the audit committee is often the de facto option for delegating the responsibility for cybersecurity risk oversight.

Focusing on the last question of analyzing the consequences of a cybersecurity breach event, the study examines the effects of having oversight (and who has responsibility for such oversight) on how firms react to a cybersecurity breach event. Focusing on breach events where a firm has explicitly indicated its oversight responsibility assignment *before* the breach incident, the study tests three consequences of cybersecurity breaches; namely, the time to breach announcement, the time to breach resolution, and the frequency of a breach. The findings indicate

that the presence of oversight decreases the time firms take to announce the breach by 2.4 days as well as the time firms take to resolve the breach by 8 days. Moreover, cybersecurity risk oversight reduces the frequency of breach by 1.2 breaches. Hence, explicitly assigning cybersecurity oversight responsibility provides tangible economic benefits to a firm.

Further analysis reveals that while audit committee oversight is more effective for the timeliness of breach announcement and resolution, the full board oversight is more effective for reducing the recurrence of breaches. Overall, these findings may reflect the full board's capacity to cultivate a robust cybersecurity culture and its power to allocate adequate resources towards preventing the recurrence of cybersecurity breaches. In contrast, the observed effect of the audit committee on timely breach announcement and resolution may be attributable to its heightened involvement in risk management activities and internal controls, which grants it a more direct operational impact in this case than the full board.

Finally, to address endogeneity concerns, robustness tests for omitted variables and self-selection bias are performed. The main findings of cybersecurity risk oversight assignment and governance determinates are robust for firms' past breach experience, spillover peers breach effect, quality of corporate governance, and technological capability. Moreover, propensity score matching analysis confirms that the main findings of the relation between cybersecurity risk oversight and breach consequences are robust to alternative matching techniques.

The study makes the following contributions. First, it complements an emerging stream of cybersecurity governance literature. Namely, Lowry et al. (2021) who used an interview-based field study to examine *how* cybersecurity oversight is carried out and conclude that board cyber expertise impacts oversight effectiveness; McGrath et al. (2021) who examine the governance of cybersecurity using four case studies and report that cyber risk governance is reformed following

a cyber-attack; and Klein et al. (2022) who investigate the change in boards' cybersecurity risk oversight within the context of General Data Protection Regulation (GDPR) and document that boards of GDPR-impacted US firms increase cyber oversight assignment to the board or to a board committee. However, this study differs from these prior studies for the following reasons. The study focuses on *who* is responsible for cybersecurity risk oversight using firms' explicit disclosure in their SEC filings, hence it provides insights on the board oversight role with respect to cybersecurity risk. In particular, the study findings shed light on the evolution of cybersecurity risk oversight as an integral part of corporate governance, its evolution over time, its variation across industry sectors, and the most frequently used board/committee level cybersecurity risk oversight responsibility assignments. Furthermore, the study focuses on both the governance determinants of cybersecurity risk oversight assignment and the impact of such assignment on the economic consequences of a cyber breach event. While the study focuses mainly on boards' cybersecurity risk oversight, it also contributes to the broader corporate governance literature (Adams and Ferreira 2008; Akbas et al. 2016; Cheng et al. 2021) and particularly to the risk governance literature (Baxter et al. 2013; Beasley et al. 2021a; Beasley et al., 2021b; Beasley et al. 2022) by explicating the determinants and consequences of a specific type of risk – cybersecurity risk.

Second, the study answers the calls for examining the role of the board-level committees on cybersecurity risk oversight (Lankton et al. 2021) and the distribution of oversight responsibility between board sub-committees and the full board (Price and Lankton 2018). In this respect, the study contributes to the cybersecurity literature in two ways: identifying governance determinants that are relevant to the oversight assignment and those that are more related to the way oversight is distributed between the full board and board-level committee(s).

Third, the study illuminates how oversight assignment impacts the economic consequences of cybersecurity breaches. While some prior research examines the impact of cybersecurity incidents on different stakeholders, the stock market, and the economy (Eisenbach et al. 2022; Haislip et al. 2019), another assesses the impact of the presence of a specific committee on the likelihood of breaches or reporting of such breaches (Higgs et al. 2016; Kamiya et al. 2021), the current study explores the effectiveness of the board and/or board-level committee(s) oversight on *actual* breach outcomes in terms of timeliness of breach disclosure, resolution, and recurrence. Hence, the study deepens the understanding of the effectiveness of governance structures on cyber risk outcomes.

Fourth, the study also contributes to the literature on issues of cybersecurity disclosure (Amir et al. 2018; Ashraf 2021; Ashraf and Sunder 2023; Florackis et al. 2023; Nordlund 2019). In its recent proposed rule, the SEC specifically stated that "We are also proposing to add new Item 106 of Regulation S-K that would require a registrant to […] require disclosure about the board's oversight of cybersecurity risk, …" (SEC 2022 p. 12). Hence, cybersecurity risk governance and disclosure continue to be a high priority for SEC rulemaking (SEC 2022, 2021). The findings of the study suggest that board explicit cybersecurity risk oversight is an effective mechanism in the event of a cybersecurity breach and thus provides useful input to regulators.

Finally, the study provides practical implications. It offers timely and relevant evidence to understand cybersecurity oversight leading practices. Specifically, the study highlights the managerial implications of not only setting the right tone at the top for oversight responsibility, but also carefully choosing the oversight governance structure that best fits the board characteristics.

## 3.2 Background and hypotheses development

### 3.2.1 Institutional background

The SEC started requiring firms to include material risk information under the Risk Factor Disclosure in their 10-K reports in 2005 (SEC 2005), without explicitly mentioning cybersecurity risks. The increase in the number and impact of cyber-attacks since then led the SEC to issue cybersecurity disclosure guidance in 2011 (SEC 2011) and an update to assist public companies in preparing and reporting their cybersecurity disclosures to investors (SEC 2018). In addition, the SEC is currently evaluating a proposed rule that aims to require, among others, public companies to provide periodic disclosures about board oversight of cybersecurity risk (SEC 2022). In addition, many professional bodies issued cybersecurity-related policies, procedures, guidelines, and frameworks (AICPA 2018; COSO 2015; IIA 2016; ISO 2013; NIST 2018; PCAOB 2018).

The SEC proxy disclosure enhancements mandate the role of the board in risk oversight (SEC 2009), requiring registrants to disclose how the board administers its risk oversight function. Although these enhancements do not mandate any particular risk oversight structure, they stipulate that "risk oversight is a key competence of the board". Furthermore, "disclosure about the board's involvement in the oversight of the risk management process should provide important information to investors about 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". The board's specific role in *cybersecurity risk oversight* was clearly underscored by the SEC's Commissioner: "[w]hen considering the board's role in addressing cybersecurity issues, it is useful to keep in mind the broad duties that the board owes to the corporation and, more specifically, the board's role in corporate governance and overseeing risk management" (Aguilar 2014). More fundamentally, the board's responsibility for cybersecurity risk oversight evolves from the "duty of oversight" and is

grounded in the fiduciary obligations of directors (Landefeld et al. 2015). However, there is no due care standard or regulatory guidance that boards can follow to fulfill their cybersecurity risk oversight obligations (Loop 2016). Hence, it is left to the board to determine how to effectively undertake its responsibility of cybersecurity risk oversight.

### 3.2.2 Relevant literature and hypotheses development

Cybersecurity risk oversight has been mainly discussed in professional literature and relatively recently in academic literature. For example, a recent discussion with boards reveals lack of agreement on a unified form of oversight structure (Sumner et al. 2020), scarcity of cyber resiliency and readiness disclosure, and increasing assignment of oversight to the audit committee (59 percent in 2018, 62 percent in 2019, and 67 percent in 2020 (Klemash et al. 2020)). Recently, Lowry et al. (2021) conducted an interview-based field study to examine how cybersecurity oversight is carried out, finding that board expertise in cybersecurity has a significant impact on oversight outcomes. Similarly, McGrath et al. (2021) employed a case study approach to examine cybersecurity governance, observing that the aftermath of a cyber-attack leads to reform in cyber risk governance. Furthermore, Klein et al. (2022) conducted a study of GDPR-impacted US firms, finding that these firms experienced a notable increase in the assignment of cybersecurity risk oversight responsibility to the board or a board committee. However, cybersecurity risk oversight still struggles to find a home in the boardroom, and boards continue to shift responsibility for oversight of cybersecurity risk between the full board and board-level committees (PwC 2018). Hence it is clear that there is no common practice on who should oversee cybersecurity risk or what is the association between different oversight setups and the consequences of cybersecurity breaches.

On the one hand, there is a view that the full board should oversee cybersecurity risk and not delegate that to a committee, a view that can be understood in the context of efficiency considerations. In such a case, however, the board needs to appoint a cyber-savvy director to lead cybersecurity risk and resilience issues and the recruitment of directors with cybersecurity expertise (Rothrock et al. 2018). However, IT-savvy directors are rare and represent only 1 percent of directors (SpenserStuart 2016). On the other hand, there are many factors that constrain the full board involvement in the oversight of cybersecurity risk, leading the board to delegate it to a board-level committee (Price and Lankton 2018). Such factors include low board knowledge and experience with IT (Coertze and von Solms 2014; Turel and Bart 2014) and low level of importance assigned to IT in the organization (Nolan and McFarlan 2005), a view that can be understood from a competency lens.

Some practitioners argue that what is important is not who oversees cybersecurity risk, rather it is the existence of an integrated approach to prepare, protect, detect, and respond to cyber incidents (KPMG 2016). Given the absence of legislative or empirical guidance on where to position cybersecurity risk oversight in the organization, it is an empirical question to examine where cybersecurity risk oversight resides.

*3.2.2.1 Oversight determinants*

Research on the likelihood of cybersecurity breaches and board size is mixed. Wang and Hsu (2013) and Hsu and Wang (2014) show that board size is negatively associated with the likelihood of breaches. However, Lending et al. (2018) document that firms with smaller boards are less likely to be breached. Accordingly, the study expects that board size may influence the assignment of cybersecurity risk oversight responsibility. This leads to our first hypothesis:

> **Hypothesis 1a:** *There is an association between board size and the assignment of cybersecurity risk oversight responsibility.*

Board cybersecurity competency and expertise are important precursors for fulfilling the cybersecurity risk oversight responsibility (Ferracone 2019; Klemash et al. 2020; Landefeld et al. 2017; Sumner et al. 2020) and an important determinant of oversight effectiveness (Lowry et al.'s 2021). The significance of cybersecurity experience and expertise is demonstrated by the pending bill before Congress, which directs the SEC to issue final rules that require a publicly-traded company to "disclose in its mandatory annual report or annual proxy statement whether any member of its governing body has expertise or experience in cybersecurity; and if no member has such expertise or experience, describe what other company cybersecurity aspects were taken into account by the persons responsible for identifying and evaluating nominees for the governing body" (US Congress 2021). Prior research documents the positive impact of technology experience on the effectiveness of committee performance. For example, an audit committee with technology experience is positively associated with the technology oversight role (Hadden et al. 2003) and is negatively associated with likelihood of breaches (Chen et al. 2022). Thus, the study hypothesizes that board cybersecurity competency is likely associated with the assignment of oversight responsibility.

**Hypothesis 1b:** *There is an association between board cybersecurity competency and the assignment of cybersecurity risk oversight responsibility.*

Directors' networks facilitate the diffusion of information and experience. Firms with more connected boards make better corporate decisions (Fang et al. 2021; Larcker et al. 2013). Directors, through their networks, may be exposed to cybersecurity risk information, practices, and thus transfer knowledge gained from data breach experience to their other boards (Nordlund 2019). However, a well-connected board might be a busy board paying less attention to monitoring and advising top management (Adams and Ferreira 2008). Thus, the study hypothesizes that board

network size is likely related to the assignment of cybersecurity risk oversight responsibility leading to the third hypothesis:

> **Hypothesis 1c:** *There is an association between board network size and the assignment of cybersecurity risk oversight responsibility.*

Although gender heterogeneity has a positive influence on cybersecurity disclosure (Radu and Smaili 2021), gender-diverse boards may generate conflict and discord among board members, adversely influencing the quality of board decisions (Baker et al. 2020). Moreover, Lending et al. (2018) find firms with more gender-diverse boards are positively associated with the occurrence of a breach. Thus, the study posits that board gender diversity is likely related to the assignment of cybersecurity risk oversight responsibility, leading to the fourth hypothesis:

> **Hypothesis 1d:** *There is an association between board gender diversity and the assignment of cybersecurity risk oversight responsibility.*

Several studies argue that boards' equity ownership speaks to better alignment of their interest with that of shareholders, and thus incentivizes boards to exercise a closer oversight and control of management. In the context of cybersecurity, studies document the existence of insider trading activities of breached firms (Chen et al. 2019; Lin et al. 2020), demonstrating the value the board assigns to their wealth. However, boards with equity ownership may not commit to cybersecurity matters and oversight since the impact of cyber-attacks may be viewed as a normal cost of business (Campbell et al. 2003), and breach costs are born by other parties such as business partners, customers, and insurance (Gordon et al., 2018; Richardson et al., 2019). Hence, the study hypothesizes that board equity holding is likely associated with the assignment of oversight responsibility, leading to the fifth hypothesis:

> **Hypothesis 1e:** *There is an association between board equity ownership and the assignment of cybersecurity risk oversight responsibility.*

*3.2.2.2 Oversight consequences*

The timing of the announcement is a crucial decision by firms that suffer a data breach (Jaeger 2012). SEC cybersecurity guidance stipulates that "public companies take all required actions to inform investors about material cybersecurity risks and incidents in a timely fashion" (SEC 2018). However, this may not always be possible as most cyber breaches go unnoticed for some time, and some are never even detected. Only a minority of breaches (about one-third) is discovered within days of its occurrence (Brese 2015). On average, it takes about 206 days for a data breach to be discovered, and 314 days for it to be contained (IBM 2020).

On the one hand, the economic consequences of information security breaches are considered trivial over the long run (Campbell et al. 2003; Richardson et al. 2019), and thus managers may not take quick and meaningful remedial actions to resolve the underlying problems or strengthen IT security controls as they perceive the cost of breaches as a normal cost of business (Campbell et al. 2003). In addition, companies may withhold severe data breach news as long as possible to avoid the adverse market impact of such news (Amir et al. 2018). Sometimes, delayed disclosure may be intentional to avoid jeopardizing law enforcement's efforts (Gwebu et al. 2018), or to avoid creating further vulnerabilities because of the disclosure.

On the other hand, companies may hasten to announce and resolve data breaches to signal board and managerial effectiveness, corporate transparency, and to protect against legal and regulatory risks. In addition, the longer the wait the higher the economic, reputational, legal damages, and, consequently, the costlier the remediation (Higgs et al. 2016). Furthermore, Cheng and Walton (2019) document that delaying initial breach disclosure unfavorably impacts the investment judgment and may indicate a potentially destructive strategy for the breached company. The shorter the duration between the time of breach announcement and the time of breach resolution may reflect a firm's cybersecurity resilience. Tsen et al. (2020) highlight that the

presence of a dedicated cybersecurity organizational role is a key factor in a firm's cybersecurity resilience. Hence, the study hypothesizes that board cybersecurity risk oversight is likely related with the time to both breach announcement and resolution.

> **Hypothesis 2a:** *There is an association between board cybersecurity risk oversight responsibility and the time to both breach announcement and resolution.*

The frequency of cybersecurity breaches is an important consideration for many reasons including, its adverse impact on a firm's market value (Schatz and Bashroush 2016), on management competence and ability to exercise effective oversight (Church and Schneider 2016), and the probability of future cyber-attacks. Contrary to Schatz and Bashroush (2016), Berkman et al. (2018) report that company valuations are higher for firms that have previously experienced a cyber breach incident due to their corrective value-enhancing actions and measures to minimize the likelihood of future breaches. While Amir et al. (2018) find an insignificant impact of multiple cyber-attacks, Jiang et al. (2021) indicate that initial and subsequent breaches affect a firm's additional reporting of cybersecurity risks disclosures. Hence, board cybersecurity risk oversight is likely related to the frequency of cybersecurity breaches.

> **Hypothesis 2b:** *There is an association between board cybersecurity risk oversight responsibility and the frequency of cybersecurity breaches.*

## 3.3 Research design

### 3.3.1 Sample selection

The study obtains cybersecurity risk oversight responsibility from proxy statements (DEF 14A), financial data from Compustat, board-level data from BoardEx, and cybersecurity breach events from Advisen Ltd. To examine the determinants and consequences of cybersecurity risk oversight, the sample includes incidents of U.S. publicly listed firms that suffered a data breach

for the period 2010 to 2020; a total of 13,932 cybersecurity breach events for 1,815 unique firms. Panels A of Table 1 presents cybersecurity breach event sample selection.

…….. [Insert Table 1 about here] ……...……...

To address the question of where cybersecurity risk oversight (*OVERSIGHT*) is assigned and observe some of its trends, the proxy statements (DEF 14A) filings are collected from the SEC's EDGAR database for the U.S. publicly listed breached firms for the period 2010 to 2020. The term "*cyber*" is searched for in the proxy statements. This search strategy is general and comprehensive. There are 2,814 proxy statements with the term "*cyber*" regardless of frequency or being standalone or part of a compound term like "*cybersecurity*". Each of these proxy filings is manually examined to determine the oversight responsibility for cybersecurity. Appendix A - section A provides examples of search results, and Panels B and C of Table 1 present the sample selection and distribution by industry for the main oversight sample.

The study classifies each case based on whether oversight is the responsibility of the full board, a specific committee, or multiple committees and eliminates irrelevant results.[12] There are 2,174 proxy statements having a clear cybersecurity risk oversight responsibility assignment. The classification generates ten categories of oversight: full board, committee (audit, finance, technology, compliance, risk, joint, cybersecurity, nominating and governance, and other). When the assignment to a specific committee is not clear, the responsibility is assigned to the full board

[12] Examples of irrelevant results of the term "*cyber*" include: 1) when it is used in reference to the name of a company as in the case of Wright Express Co.'s DEF 14A (2011) mentioning "Cybersource Corp." as one of the peer companies; 2) when it used as board member background as in "From 2000-2001, he was president and chief operating officer of CyberSafe Corporation, a global security software provider, where he was responsible for the overall financial services and operations of the company" (ACXIOM Co.'s DEF 14A (2017)); 3) when it is used to indicate cyber fees as in "All other fees include primarily advisory services related to other process assessments and consulting assistance related to our cybersecurity readiness program in fiscal year 2015" (MSC Industrial Direct Co. Inc. DEF 14A (2016)); or 4) when it mentioned as a type of risk as in "we face a number of risks, including economic risks, financial risks, legal and regulatory risks, cybersecurity risks and others" (Sensata Technologies Holding DEF 14A (2019)).

because per the SEC the ultimate risk responsibility rests on the full board.[13] This oversight assignment process is deterministic as it is based on what is explicitly mentioned in the proxy statements and does not rely on the classifier's judgment.

To simplify the analysis, the ten classifications are grouped into three categories: full board, audit committee, and non-audit committee; based on the rationale of whether firms deem the responsibility of oversight rests with the full board or should be assigned to a board-level (audit or non-audit) committee. The oversight may be under the purview of the audit committee, which has responsibility over risk oversight (NYSE 2021; Yew et al. 2015) and compliance with the Sarbanes-Oxley Act (Gordon et al. 2006).[14] Lawrence et al. (2018) link cybersecurity incidents to potential internal control weaknesses; and Lankton et al. (2021) find that prior data breach, in the presence of a technology committee, increases the likelihood that a firm will assign cybersecurity governance role to the audit committee. Moreover, the evolving nature of cybersecurity risks may lead some firms to assign oversight responsibility to a non-audit committee, reflecting a firm's specific operation or industry affiliation. For example, "companies with strategic interests in IT or those that would benefit from a sharp governance focus on cybersecurity and cyber risk" may assign oversight responsibility to cybersecurity committee (Sumner et al. 2020).

[13] For example, BioTelemetry, Inc. in its 2017 DEF 14A discloses that "The Board's Role in Risk Oversight […] While the Chief Executive Officer, the General Counsel and other members of our senior leadership team are responsible for the day-to-day management of risk, our Board is responsible for ensuring that an appropriate culture of risk management exists within our company and for setting the right "tone at the top," overseeing our aggregate risk profile, and assisting management in addressing specific risks, such as strategic and competitive risks, financial risks, brand and reputation risks, legal risks, regulatory risks, operational risks and cybersecurity risks".

[14] Although, SOX does not explicitly address the issue of cybersecurity, firms' financial reporting systems, which are required to comply with SOX, are based on sophisticated computer-based systems, implying the importance of information security (Gordon et al. 2006) and that reliable and transparent financial reporting are contingent on secure computer-based information systems (Gordon et al. 2015). In addition, Gordon et al. (2006) also argue that: "In a modern computer-based environment, firms cannot produce reliable financial reports without having secure computer systems".

3.3.2 Models and variable measurement

The study estimates the following logistic regression to investigate governance determinants of the board's cybersecurity risk oversight assignment:

$$OVERSIGHT_{i,t} = \beta_0 + \beta_1 BOARD\_SIZE_{i,t-1} + \beta_2 COMPETENCY_{i,t-1} + \beta_3 NETWORK\_SIZE_{i,t-1} + \beta_4 GENDER\_DIVERSITY_{i,t-1} + \beta_5 EQUITY\_HOLDING_{i,t-1} + \sum_{j=1}^{k} \beta_j CONTROL_{j,t-1} + \lambda_1 YearFixedEffects + \lambda_2 IndustryFixedEffects + \varepsilon_{i,t} \quad (1)$$

The main dependent variable is $OVERSIGHT_{i,t}$, representing the board or board committee(s) responsible for overseeing cybersecurity risk in firm *i* in year *t.* There are two categories of oversight: full board and board-level (audit or non-audit) committee. Thus, the study investigates governance determinants of oversight based on these categories in three hierarchical levels. At the highest level, it examines determinants of oversight based on the full sample in which $OVERSIGHT_t$ is defined as a binary variable equal to one for firms with an explicit cybersecurity risk oversight assignment and zero otherwise. At the next level, it examines oversight determinants for firms that have oversight where $OVERSIGHT_t$ is one for firm's that assigned oversight to the full board and zero for those firms that assigned it to a board-level committee. At the final level, the study focuses on board-committee oversight, where it explores governance determinants of $OVERSIGHT_t$, defined as one for firms that assigned cybersecurity risk oversight to audit committee and zero for those firms that assigned it to a non-audit committee.

The independent variables are governance determinants including board size ($BOARD\_SIZE_{t-1}$), measured as the number of board members, and board cybersecurity competency ($COMPETENCY_{t-1}$), measured as a percentage of directors with cybersecurity/IT competency and experience as defined by Ashraf (2020b) and Benaroch and Chernobai (2017). Moreover, board network size ($NETWORK\_SIZE_{t-1}$), defined as the natural log of the

aggregation of connections of all directors from the BoardEx database (Akbas et al. 2016). This measure of board networks simply counts the number of first-degree links for all directors on the board. Board gender diversity ($GENDER\_DIVERSITY_{t-1}$), measured as percentage of female directors, and board equity ownership ($EQUITY\_HOLDING_{t-1}$), measured as the natural log of the aggregation of board members equity ownership.

The study controls for firm size ($SIZE_{t-1}$) and various performance measures including profitability ($ROA_{t-1}$), loss ($LOSS_{t-1}$), leverage ($LEVERAGE_{t-1}$), sales growth ($SALES\_GROWTH_{t-1}$), and financial distress ($Z\_SCORE_{t-1}$), as larger and more successful firms are more target of cyber-attacks (Higgs et al. 2016). Moreover, it controls for firm age ($FIRM\_AGE_{t-1}$) as Caluwe and De Haes (2019) find a negative relationship between the firm age and board information technology governance. The study also controls for firm complexity (number of business ($SEGMENTS\_B_{t-1}$) and geographic segments ($SEGMENTS\_G_{t-1}$), whether a firm has foreign operations ($FOREIGN_{t-1}$), participates in a merger or acquisition ($ACQUSITION_{t-1}$), or restructuring ($RESTRUCTURE_{t-1}$). At the industry level, the study controls for differences in exchange requirements using a dummy variable for NYSE ($NYSE_{t-1}$), which equals one if a firm is listed on the NYSE in that year, and zero otherwise (Huang et al. 2009). Since cybersecurity breach cost and frequency differ by firm's industry affiliation, the study controls for cyber risk ($CYBER\_RISK_{t-1}$) (Ashraf 2021). The model incorporates year and industry fixed effects. Appendix B summarizes all variable definitions.

The following OLS model captures the effect of cybersecurity risk oversight on how firms react to cybersecurity breach events:

$$BREACH\_CONSEQUENCE_{i,t} = \beta_0 + \beta_1 OVERSIGHT\_PREBREACH_{i,t-1} + \beta_2 BREACH\_TYPE_{i,t} + \beta_3 INFORMATION\_TYPE_{i,t} + \beta_4 NUM\_RECORDS_{i,t} + \beta_5 ACTORS_{i,t} + \beta_6 SOURCE\_OF\_ATTACK_{i,t} +$$

$$\sum_{j=1}^{k} \beta_j CONTROL_{j,t-1} + \lambda_1 YearFixedEffects + \lambda_2 IndustryFixedEffects + \varepsilon_{i,t} \quad (2)$$

The study examines the impact of pre-breach cybersecurity risk oversight ($OVERSIGHT\_PREBREACH_{t-1}$), a binary variable equal to one for firms with an explicit oversight assignment *before* the breach incident and zero otherwise, on the three consequences of a breach event. First, the time to breach announcement ($TIME\_TO\_ANNOUCEMENT_t$), defined as the number of days between incident date and first notice date. Second, the time to breach resolution ($TIME\_TO\_RESOLUTION_t$), defined as the number of days between original loss start date and original loss end date. Third, the recurrence of breach ($BREACH\_FREQUENCY_t$), calculated as number of breach events(s) encountered by the breached firm. The study incorporates a set of cyber breach characteristics in Equation (2) using Advisen's representations for these characteristics including breach type ($BREACH\_TYPE_t$) and types of data, assets, or information that is compromised ($INFORMATION\_TYPE_t$), an indicator variable for whether cybersecurity breach event is perpetrated by internal or external actors ($ACTORS_t$), number of records lost ($NUM\_RECORDS_t$), and the source of the breach ($SOURCE\_OF\_ATTACK_t$). The study also controls for the firm and industry characteristics and incorporates year and industry fixed effects. Appendix B lists variable definitions.

3.3.3 Descriptive statistics and correlations

Table 2 shows summary statistics for the oversight sample (the first level i.e., whether there is oversight or not). Panel A reports that there are 29 percent of firm year observations reporting the existence of $OVERSIGHT$ assignment. The average board size is 10, mostly (83 percent) male directors, with an average network size of over 1000. In addition, the firms have positive sales growth and an average age of 30 years. Panel B presents that while there are 16 percent of firms

years observations that assign the oversight to full board versus board-level committee, 58 percent of firms years observations assign it to audit committee versus non-audit board-level committee.

…….. [Insert Table 2 about here] ……...……...

Table 3 provides Pearson correlations for the oversight sample. The presence or lack of oversight is significantly positively ($p$-value ≤ 0.01) correlated with a board size (coefficient of 0.14), competency (coefficient of 0.07), network size (coefficient of 0.22), and board equity holding (coefficient of 0.17), and negatively correlated with board gender diversity (coefficient of -0.26). Moreover, oversight is highly positively correlated with firms with business and geographic segments with coefficients of 0.37 and 0.33 respectively.

…….. [Insert Table 3 about here] ……...……...

**3.4 Analysis and results**

**3.4.1 Who is in charge of cybersecurity risk oversight?**

This section provides insights on exploratory analysis of where the responsibility of cybersecurity risk oversight rests based on the ten possibilities derived from inspection of proxy statements: full board, audit committee, finance committee, technology committee, compliance committee, risk committee, joint committee, cybersecurity committee, nominating and governance committee, and "other" committee. Panel A of Table 4 provides frequency (percentage) of whether firms disclose their cybersecurity risk oversight responsibility assignment or not. Most firms (71 percent) do not disclose the board role in cybersecurity risk oversight in their proxy statements. Of the firms that explicitly assign cybersecurity risk oversight responsibility, 83 percent (17 percent) disclose that at least one board-level committee (the full board) is charged with oversight of cybersecurity matters. When firms assign oversight responsibility to a board-level committee, most (57 percent) delegate it to the audit committee, about 11 percent to the risk committee, about 5

percent to the technology committee, and few (2 percent) charge the role to a focused cybersecurity committee. Possibly to better distribute the board's workload, some firms assign oversight responsibility role to a joint committee (3 percent), nominating and governance committee (1 percent), or "other" committees.

Panel B presents the preference of cybersecurity risk oversight assignment across industry sectors. Most industries prefer to assign the oversight responsibility to the audit committee followed by the full board. Firms in "Energy, Oil, and Gas" and "Chemical and Allied Products" industries demonstrate the least variations in oversight assignment. Oversight in firms in the sectors of "Finance" and "Computers, Software, and Electronic Equipment" permeate all possible assignment options followed by "Wholesale and Retail", "Healthcare", and "Utilities" industries. Overall, the most common oversight assignments are the audit committee followed by the full board for all sectors, except for the "Finance" sector it is audit committee followed by risk committee and the "Consumers Durables" sector it is audit committee followed by technology committee.

Viewing classification of cybersecurity risk oversight role in high versus low regulated categories (IBM 2020), the study finds that there is wide variation among both categories, reflecting the effects of high regulation and the associated legal costs. Moreover, the analysis reveals that some firms (5 percent in the sample) shift oversight responsibility from a board or board committee(s) to another. For example, whereas Johnson & Johnson in 2018 shifts cybersecurity risk oversight role away from the Audit committee to Regulatory Compliance Committee, Fortinet Company in 2019 shifts the oversight role from the full board to the Audit committee. While some firms mention the reasons for the shift (reducing the burden on audit committee, in response to a cybersecurity breach, or for better oversight focus), others do not.

It is worth noting that some firms went beyond disclosure of who's responsible of cybersecurity risk oversight and provided details on how they carry out cybersecurity risk oversight responsibility. For example, disclosure details include information about cybersecurity periodic reviews and updates, who leads cybersecurity mitigation program, the existence of enterprise risk management framework, use of independent cybersecurity consultant, education and training, and number of meetings with CIOs, among others (see Appendix A – section B).

Figure 1 shows cybersecurity risk oversight responsibility assignment over the years. Firms started to assign oversight responsibility around 2012, shortly after the SEC 2011 cybersecurity guidance, with an upward trend over the years. Furthermore, there is a major increase (117 percent) of oversight assignment in 2018 compared to 2017, that may reflect the effect of the SEC February-2018 cybersecurity interpretive guidance. The disclosure on cybersecurity reflected using the term "cyber" in the proxy statements also demonstrates similar but higher time trend.

The overall findings concur with the position of the SEC of leaving who oversees the cybersecurity risk to the board to decide. Although the audit committee is a popular choice, there is a wide variation of cybersecurity risk oversight responsibility assignment, possibly reflecting the varying particularities of firms as anticipated by the regulator.

…….. [Insert Table 4 about here] ……...……...

…….. [Insert Figure 1 about here] ……...……...

**3.4.2 Determinants of cybersecurity risk oversight responsibility assignment**

This section investigates the association between firm's governance characteristics and cybersecurity risk oversight assignment using different samples (Equation 1). First, the study explores governance characteristics as determinants of whether firms explicitly assign cybersecurity risk oversight responsibility or not. Then, it examines the governance determinants

for the firms that assign responsibility of oversight, whether to the full board or to a board-level committee(s). At a more granular level, the study examines governance determinants for firms that assign oversight to audit committee or non-audit committee.

*3.4.2.1 Level 1: Did firms assign cybersecurity risk oversight responsibility or not?*

Table 5 summarizes the regression results for the governance determinants of cybersecurity risk oversight location for level 1 sample, where $OVERSIGHT_t$ is defined as one for firm $i$ in year $t$ with an explicit cybersecurity risk oversight assignment and zero otherwise. Column (1) presents results without controls and fixed effects, Column (2) presents results with fixed effects, and Column (3) reports results with controls and fixed effects. Across the three columns, board cyber competency, network size, and gender diversity are significantly related with the oversight assignment. Focusing on Column (3), the coefficients of board cyber competency and network size are positive (2.687, $p$-value $\leq 0.001$ and 0.703, $p$-value $\leq 0.001$, respectively), suggesting a positive relation between board cyber competency and network size and oversight assignment. It appears that directors' cyber competency and connections increase the board's overall awareness of cybersecurity risks and issues, which, in turn, motivates the board to explicitly disclose their oversight assignment. This finding agrees with that of Nordlund (2019), namely directors transfer knowledge gained from data breach experience via connection to their other boards and substantiates the SEC's 2022 proposed rule for board cyber competency disclosure.

The coefficients of board equity holding and their gender diversity are significant and negative (-0.016, $p$-value $\leq$ 0.1; -1.291, $p$-value $\leq$ 0.001, respectively), indicating that the more equity holding and gender-diverse the board is, the less likely the board will explicitly assign cybersecurity risk oversight. The negative association between board gender diversity and cybersecurity risk oversight indirectly confirms Lending et al. (2018) finding that firms with more

gender-diverse boards (with less attention to explicit oversight responsibility assignment) are positively associated with the occurrence of a breach; and contradicts that of Radu and Smaili (2021) where board gender diversity is positively associated with cybersecurity disclosure. The negative association between board equity holding and explicit cybersecurity risk oversight assignment may reflect the short-lived market impact of breach incidents (Richardson et al. 2019).

Furthermore, it appears that a firm's board size does not play a role in determining whether a firm discloses on oversight or not. About the control variables, a firm's characteristics in terms of size, leverage, restructuring, having foreign operations, and NYSE-listing status are significant and positively related to oversight assignment. It also appears that firms with business acquisition are less likely to disclose the oversight assignment.

…….. [Insert Table 5 about here] ……...……...

*3.4.2.2 Level 2: When firms assign cybersecurity risk responsibility, do they assign it to the full board or to a board committee?*

Focusing on the sample with clear designation of cybersecurity risk oversight assignment, Table 6 reports the logistic regression results for the governance determinants of whether firms assign cybersecurity risk oversight to the full board or to a board-level committee. Across all Columns, board size is statistically significant. Based on Column (3), the study finds significant negative coefficient of -0.086 ($p$-value $\leq 0.05$) on board size, suggesting that an additional director to the average board of about 10 members would be associated with an 8.6 percent decrease of oversight assignment to the full board. This finding supports the notion that the bigger the board size is the more reasonable the assignment of oversight to a board-level committee for closer oversight and inspection of cyber risks and issues. Firm size and geographic segments are negatively and significantly related to the full board cybersecurity risk assignment, but firm age,

profitability, loss, and business segments are positively related to the full board oversight assignment. For industry control, while firms listed on NYSE have a significantly negative effect (-0.233, *p*-value ≤ 0.1), operating in vulnerable industry has a significantly positive impact (0.382, *p*-value ≤ 0.05) on assignment cybersecurity risk oversight to the full board.

…….. [Insert Table 6 about here] ……...……...

*3.4.2.3 Level 3: When firms assign cybersecurity risk responsibility to a board committee, do they assign it to the audit committee or non-audit committee?*

Table 7 provides logistic regression results. The analysis reveals that board size, cyber competency, and equity holding are significant across all Columns. Specifically, in full model (Column (3)), while board cyber competency (3.499, *p*-value ≤ 0.1) and equity holding (0.105, *p*-value ≤ 0.001) are significant and positively associated with audit committee oversight assignment, board size and their connections are negatively associated with such assignment. This finding indicates that increasing board cybersecurity experience and equity holdings reduces the odds of assigning the oversight responsibility to the non-audit committee. The positive association possibly signifies that boards with more stake in the organization (i.e., wealth involvement) will prefer to relegate the oversight to the audit committee. Moreover, the directors' domain knowledge of cybersecurity threats and issues influences their decision of oversight assignment in favor of the audit committee. On the other hand, the smaller the board with less connections the higher likelihood that audit committee will oversee the cybersecurity risk. This finding supports the organizational efficiency view. With respect to firm characteristics, namely, profitability, loss, leverage, growth, age, and business segments (firm size) are significant and positively (negatively) associated with the assignment of oversight to audit committee.

…….. [Insert Table 7 about here] ……...……...

### 3.4.3 Consequences of cybersecurity risk oversight assignment

This section studies the relation between oversight and a firm's response to cybersecurity breaches (Equation 2), focusing on breach event observations where a firm has an explicit cybersecurity risk oversight assignment *before* the cybersecurity breach incident. The study tests three consequences of cybersecurity breaches: namely, the $TIME\_TO\_ANNOUCEMENT_t$, $TIME\_TO\_RESOLUTION_t$, and $BREACH\_FREQUENCY_t$. Table 8 reports the descriptive statistics for data breach sample. Panel A indicates that the average time to the breach announcement is 137 days, and the average time to the breach resolution is 156 days. The average frequency of breach event is11.25. Panel B reports descriptive for class variables. 61% of the $BREACH\_TYPE_t$ relates to data and 67% of $SOURCE\_OF\_ATTACK_t$ is associated with firms *SEVER_CLOUD_WEB*.

…….. [Insert Table 8 about here] ……...……...

Table 9 reports Pearson correlations for data breach sample. That table shows that cybersecurity risk oversight is positively (negatively) correlated with time to breach announcement (breach frequency). While type of information loss is positively related with all breach consequences, number of records lost is negatively related with the timeliness of breach announcement and resolution. Moreover, type of breach perpetrator ($ACTOR_t$.) is positively related to breach frequency and the time firms take to resolve the breach.

…….. [Insert Table 9 about here] ……...……...

To study the consequences of cybersecurity risk oversight assignment on the firm's response measures to the breach, the analysis is restricted to those events where oversight assignment is defined *prior* to the breach event, thus excluding events where the oversight assignment is introduced post the breach event. Table 10 presents results of OLS regression of

consequences of firms' cybersecurity risk oversight assignment on the firm's response measures to the breach. Starting with duration of the breach, Columns (1) and (2) present the relationship between cybersecurity risk oversight and the time to the breach announcement ($TIME\_TO\_ANNOUCEMENT_t$).[15] Focusing on Column (3), the coefficient of cybersecurity risk oversight is negative (-0.886, $p$-value ≤ 0.001), suggesting that oversight responsibility assignment reduces the time firms take to announce the breach. Specifically, the presence of cybersecurity risk oversight decreases time to announcement by about 2.4 days, hence highlighting the benefit that the firm gains from having an explicit oversight responsibility assignment. While breach committed by internal actors, number of records loss, and the client hardware and violations of privacy laws as source of the attack are positively associated with the duration of the breach announcement, data and privacy types of the breach, and breached financial information are negatively related with the duration of the breach announcement. The latter finding may reflect the complexity of assessing the impact of financial and privacy breaches before announcing them to the affected parties and the public. For control variables, all firms' characteristics are negatively associated with time to breach announcement.

Columns (3) and (4) show the impact of cybersecurity risk oversight on the time to breach resolution ($TIME\_TO\_RESOLUTION_t$). Across all Columns, oversight is negatively related with firms' resolution timeliness. Particularly, in Column (4), firms' cybersecurity risk oversight assignment is negatively (-2.038, $p$-value ≤ 0.001) associated with the time it takes firms to resolve a breach. This result indicates that explicit cybersecurity risk oversight decreases time to breach resolution by about 8 days, reflecting that oversight provides direction and guidance during the

[15] In untabulated tests, the results hold across the three breach consequences (*TIME_TO_ANNOUNCEMENT*$_t$, *TIME_TO_RESOLUTION*$_t$, and *BREACH_FREQUENCY*$_t$) after controlling for: prior breach experience, quality of a firm's information technology, and firms' use of cybersecurity framework.

breach incident. Observations on firms and breach characteristics indicate that privacy as breach type and source of attack involving telecom and privacy law violations, number of records, breach actor, firms' size, profitability, and reporting loss are positively related with time to breach resolution. Moreover, breach types involving data, and financial information loss, operating in high cyber risk industries are negatively related with breach resolution timeliness.

Columns (5) and (6) report the impact of negative association between cybersecurity risk oversight on breach frequency. In Column (6), the findings indicate that oversight is negatively associated with breach recurrence (-0.154, $p$-value $\leq$ 0.001), indicating that oversight reduces breach frequency by 1.2 breaches than when there isn't. This finding reflects that oversight at the board level reduces breach frequency, thus supporting Haislip et al. (2021) finding that better cybersecurity governance, resulting from executives with more IT knowledge, reduces data security breaches. The results also show that while breach type involving data and actors are positively associated with breach frequency, breach type involving privacy and source of attack relating with client hardware; server, cloud, web; and telecommunication are negatively related with breach recurrence. Finally, the number of records lost is negatively related with the frequency of breaches, suggesting that the more firms' data and information are compromised, the more preventive measures firms implement, and, consequently, the less likely breach recurrence becomes. Moreover, firms' size, leverage, and operating in high cybersecurity risk industry are positively related with breach frequency (perhaps bigger firms that are less financially constrained are more attractive targets) and reporting of loss are negatively associated with the frequency (perhaps because the financials of such firms are not attractive to data predators).

…….. [Insert Table 10 about here] ……...……...

An additional analysis is performed to examine the efficacy of full board versus audit committee oversight with respect to time to breach announcement, resolution, and frequency. The result (untabulated) shows a significant difference in the time to breach announcement between the two groups, where audit committee oversight reduces time to announcement by 1.4 days compared with that of full board. In terms of time to resolve a breach, both the full board and the audit committee contribute to an increase in the number of days, with the audit committee showing a comparatively lesser impact than the full board. Moreover, full board oversight is better than audit committee oversight for breach frequency and reduces recurrence of breaches by 1.2 breaches. These findings may indicate that the board has the capacity to muster the necessary culture and resources to defend against recurrence of breaches. On the other hand, the audit committee's effectiveness on breach timeliness may reflect its greater operational engagement in risk management activities and internal controls compared with the full board.

### 3.4.4 Additional tests

*3.4.4.1 Cybersecurity role*

While Zafar et al. (2016) and Haislip et al. (2021) report that the presence of a cybersecurity role is associated with better firm performance after information security breach incident and reduced data security breaches, respectively; Smith et al. (2021) indicate that firms disclosing the presence of a CIO/CISO are more likely to be breached. Thus, the study examines the presence of CIO/CISO role ($CYBERSECURITY\_ROLE_t$) on whether firms assign cybersecurity risk oversight or not. Table 11, Column (1) of Table 11 reports the positive relation (0.321, $p$-value ≤ 0.001) between the presence of cybersecurity role and the firm's explicit disclosure of cybersecurity risk oversight responsibility assignment. This result may indicate that presence of cybersecurity role in the organizations plays a critical role in facilitating the decision to assign oversight as it enables

cybersecurity coaching (Lowry et al. 2021). However, this relationship (untabulated) does not hold for the full board and board-level committee assignments.

*3.4.4.2 Presence of risk, compliance, or technology committees*

The study examines whether the presence of risk, compliance, and/or technology committees impacts the assignment of cybersecurity risk oversight responsibility. Prior studies show that the presence of such committees is related to the likelihood of a breach occurrence and disclosure (Higgs et al. 2016; Smith et al. 2019). Including indicators identifying firms with risk, compliance, and/or technology committees in Equation (1), the results show that the presence of such committees is indeed negatively associated with firms' explicit disclosure of oversight assignment (Column (2) of Table 11). This finding may suggest that these committees may already be handling the cybersecurity risk, thereby eliminating the need for the board to assign the oversight responsibility. This conclusion holds (untabulated) for the interaction between these committees and being in the financial industry, which may reflect the nature of the financial industry being regulated and highly targeted (IBM 2022) for amassing large amounts of data.

*3.4.4.3 The use of cybersecurity framework*

To better manage cybersecurity risks (Aguilar 2014) and to assess compliance to cybersecurity initiatives, firms may adopt a well-known cybersecurity framework (Frank et al. 2021). However, organizations may opt not to invest in these frameworks due to cost considerations and difficulty of measuring their return on investment (Moore et al. 2015). Hence, the study tests whether disclosure about the use of cybersecurity frameworks ($CYBERSECURITY\_FRAMEWORK_i$) impacts whether firms assign cybersecurity risk oversight or not. Results in Column (3) support the positive relation between frameworks' use and the firms' oversight assignment (0.511, $p$-value $\leq$ 0.1). Hence, this finding highlights that a firm's risk

management processes reflect on the tone at the top and facilitate cybersecurity risk oversight assignment. This relationship does not hold for the full board and board-level committee assignments.

*3.4.4.4 Audit committee as a default cybersecurity risk oversight assignment*

To investigate whether assignment of cybersecurity risk oversight responsibility to audit committee is not a default decision or a reflection of availability of other committees with appropriate skills to oversee the cybersecurity risks, the study examines the governance determinants of audit committee oversight assignment controlling for the presence of any one of risk, compliance, and/or technology committees ($PRESENCE\_OF\_RCT_{t-1}$). Table 11, Column (5) shows that the results stay the same after including this variable in Equation (1), thus supporting the audit committee default assignment "tradition" where "… boards have put the cyber oversight role in the audit committee and that's because that's where we're dealing with all things that involve risk" (Trautman et al. 2022).

…….. [Insert Table 11 about here] ……...……...

**3.4.5 Endogeneity issues**

To address the endogeneity issues of omitted variables that correlate with firm governance characteristics and cybersecurity risk oversight assignment, the study performs follow-up tests. First, firms are likely to assign cybersecurity risk oversight in response to spillover of peers' breach (Rosati et al. 2019; Ashraf 2021) or the likelihood of experiencing such breach. Thus, the study incorporates an indicator variable for probability of peers' breach in Equation (1). The main results (untabulated) stay the same. Second, firms with prior data breaches are more likely to assign oversight as a mitigating measure following a breach. Hence, the study controls for the firm's past data breach experience by incorporating an indicator variable and the inferences (not tabulated)

remain unchanged. Third, institutional owners, a proxy measure for firm governance quality, can improve firm's risk practices (Florackis et al. 2023). To control for such effect, an indicator of higher institutional ownership at the firm is included and the results (Column (4) of Table 11) stay the same. Finally, firms belonging to high-tech industries may demonstrate greater technical capability in discovering and resolving breaches than non-high-tech firms, hence are more likely to assign oversight. The inferences stay the same after controlling for the overall high-tech quality.

To evaluate if endogeneity is a concern in analysis of cybersecurity risk oversight and breach consequences (i.e., a potential of self-selection bias in the sample) in Equation (2), the study uses propensity score matching. Hence, a matched sample of firms with no cybersecurity risk oversight that are similar to cybersecurity risk oversight sample firms in terms of industry affiliation, size, and profitability is created. The matched sample results (not tabulated) show that endogeneity is not a concern.

### 3.5 Conclusion

The study examines the current state of board cybersecurity risk oversight, its positioning in the organization, its governance determinants, and the consequences of such positioning in the event of a cybersecurity breach. The exploratory analysis reveals a wide variation in cybersecurity risk oversight responsibility assignment including assigning it to the full board or board-level committee such as the audit, finance, technology, compliance, risk, joint, cybersecurity, nominating and governance, and others. However, most firms (57 percent) across industry sectors delegate cybersecurity oversight to the audit committee.

Using a cascading three-level analysis approach of governance determinants, the study finds, at the first level, that board's cyber experience, network size, equity ownerships, and gender diversity are significant factors of disclosure of explicit assignment of oversight responsibility.

Specifically, whereas a board's cyber experience and network size are positive determinants, equity ownership and gender diversity are negative determinants. Furthermore, the study finds that the presence of cybersecurity role and risk management framework at the management level are also significant factors of oversight assignment. At the second level of oversight analysis, the results show that smaller boards increase the likelihood that the full board will oversee cybersecurity risk as opposed to board-level committee(s). At the third level of oversight analysis, while boards with more equity ownership and cybersecurity experience tend to delegate oversight to the audit committee, bigger boards with higher network size are more likely to assign it to a non-audit board-level committee(s). Furthermore, the results confirm that the audit committee is the default option for assigning cybersecurity risk oversight responsibility when a firm has a risk, compliance, and/or technology committee. Overall, the findings of this cascading three-level analysis approach persist across financial/non-financial industry sectors, and as well when controlling for high-tech capability, governance quality, peer breach effect, and a firm's prior breach experience.

Examining the effects of cybersecurity risk oversight positioning on how firms react to cybersecurity breach events, the results indicate that the presence of pre-breach oversight reduces the time firms take to announce and to resolve breaches as well as the frequency of such breaches. These findings persist even when controlling for breach characteristics and using propensity score matching. In additional analysis, the results indicate that while audit committee oversight is more effective for the timeliness of breach announcement and resolution, the full board oversight is better for reducing the recurrence of such breaches.

The study provides empirical as well as practical contributions. The study findings contribute to the corporate governance and cybersecurity literature on the importance and the

evolution of board role in cybersecurity risk oversight. Specifically, the study reveals that governance characteristics are important drivers in firms' decision to explicitly disclose on their cybersecurity risk oversight responsibility and documents benefits of such assignment in the event of a cybersecurity breach. Practically, the study presents cybersecurity governance common practices and the relationships between board characteristics and cybersecurity risk oversight governance. Finally, the study is not without limitations. A potential limitation is that although the search strategy uses the terminology commonly used by the SEC, it may not have captured all relevant proxy statements. Moreover, the study adopts an association-based approach, and as such, the capacity to establish causal links is limited.

### 3.6 References, figures, tables, and appendices

**References**


Adams, R. B., & Ferreira, D. (2008). Do directors perform for pay?. *Journal of Accounting and Economics*, *46*(1), 154-171.

Aguilar, L. A. (2014). Boards of directors, corporate governance and cyber-risks: Sharpening the focus. In Cyber Risks and the Boardroom conference, New York Stock Exchange.

Akbas, F., Meschke, F., & Wintoki, M. B. (2016). Director networks and informed traders. *Journal of Accounting and Economics*, *62*(1), 1-23.

Aldasoro, I., Gambacorta, L., Giudici, P., & Leach, T. (2022). The drivers of cyber risk. *Journal of Financial Stability*, *60*, 100989.

American Institute of Certified Public Accountants (AICPA). (2018). Cybersecurity risk management oversight: A tool for board members. Available at: https://www.thecaq.org/wpcontent/uploads/2019/03/caq_cyber security_risk_ manag ement_oversight_tool_2018-04.pdf

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

Angst, C. M., Block, E. S., D'Arcy, J., & Kelley, K. (2017). When do IT security investments matter? Accounting for the influence of institutional factors in the context of healthcare data breaches. *MIS Quarterly, 41*(3), 893-916.

Ashraf, M., & Sunder, J. (2023). Can shareholders benefit from consumer protection disclosure mandates? Evidence from data breach disclosure laws. *The Accounting Review*, *98*(4), 1-32.

Ashraf, M., Choudhary, P., & Jaggi, J. (2020a). Audit committee oversight and financial reporting reliability: are audit committees overloaded?. Available at SSRN 3433389.

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

Ashraf., M. (2021). Should the SEC allow managers discretion when disclosing risk factors? Evidence from peer data breaches and cyber risk factors. Working paper, Available at SSRN: https://ssrn.com/abstract=3807487

Baker, H. K., Pandey, N., Kumar, S., & Haldar, A. (2020). A bibliometric analysis of board diversity: Current status, development, and future research directions. *Journal of Business Research*, *108*, 232-246.

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

Baxter, R., Bedard, J. C., Hoitash, R., & Yezegel, A. (2013). Enterprise risk management program quality: Determinants, value relevance, and the financial crisis. *Contemporary Accounting Research*, *30*(4), 1264-1295.

Beasley, M. S., Branson, B., Braumann, E., & Pagach, D. (2022). Understanding the ecosystem of enterprise risk governance. *The Accounting Review*, https://doi.org/10.2308/TAR-2020-0488

Beasley, M. S., Branson, B., Pagach, D., & Panfilo, S. (2021a). Are required SEC proxy disclosures about the board's role in risk oversight substantive?. *Journal of Accounting and Public Policy*, *40*(1), 106816.

Beasley, M. S., Goldman, N. C., Lewellen, C. M., & McAllister, M. (2021b). Board risk oversight and corporate tax-planning practices. *Journal of Management Accounting Research*, *33*(1), 7-32.

Benaroch, M., & Chernobai, A. (2017). Operational IT failures, IT value-destruction, and board-level IT governance changes. *MIS Quarterly*, *41*(3), 729–762.

Berkman, H., Jona, J., Lee, G., & Soderstrom, N. (2018). Cybersecurity awareness and market valuations. *Journal of Accounting and Public Policy, 37*(6), 508-526.

Braumann, E. C., Grabner, I., & Posch, A. (2020). Tone from the top in risk management: A complementarity perspective on how control systems influence risk awareness. *Accounting, Organizations and Society*, *84*, 101128.

Brese, F. R. (2015). Effective cyber risk management: An integrated approach. In M. Rosenquist (Eds.), Navigating the digital age (pp. 43-48). Caxton Business & Legal, Inc.

Caluwe, L., & De Haes, S. (2019). Board Level IT Governance: A scoping review to set the research agenda. *Information Systems Management*, *36*(3), 262-283.

Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: empirical evidence from the stock market. *Journal of Computer Security, 11*(3), 431-448.

Chande, N., & Yanchus, D. (2019). The cyber incident landscape. *Working paper* (No. 2019-32). Bank of Canada.

Chen, C., Hartmann, C. C., & Gottfried, A. (2022). The impact of audit committee IT expertise on data breaches. *Journal of Information Systems, 36*(3), 61-81.

Chen, X., Hilary, G., & Tian, X. S. (2019). Data breach disclosure and insider trading. Working paper. McDonough School of Business Georgetown University (Ed.), 1-37.

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

Cheng, X., & Walton, S. (2019). Do nonprofessional investors care about how and when data breaches are disclosed?. *Journal of Information Systems*, *33*(3), 163-182.

Church, B. K., & Schneider, A. (2016). The impact of Section 302 and 404 (b) internal control disclosures on prospective investors' judgments and decisions: An experimental study. *International Journal of Auditing*, *20*(2), 175-185.

Clayton, J. (2017). "Statement on Cybersecurity," (SEC, Washington DC, September 20, 2017). Available at: https://www.sec.gov/news/public-statement/statement-clayton-2017-09-20

COBIT. (2019). COBIT certification. Available at: https://www.isaca.org/credentialing/cobit

Coertze, J., & von Solms, R. (2014, January). The board and CIO: The IT alignment challenge. In *2014 47th Hawaii International Conference on System Sciences* (pp. 4426-4435). IEEE.

Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2015). COSO in cyber age. Available at: https://www.coso.org/documents/COSO%20 in%20the %20 Cyber%20Age_FULL_r11.pdf

Davis., G. (2016). Prioritizing cybersecurity: Five investor questions for portfolio company boards. Available at: https://corpgov.law.harvard.edu/2016/05/20/prioritizing-cybersecurity-five-questions-for-portfolio-company-boards/ (Accessed September 18, 2021).

Deane, J. K., Goldberg, D. M., Rakes, T. R., & Rees, L. P. (2019). The effect of information security certification announcements on the market value of the firm. *Information Technology and Management*, *20*(3), 107-121.

Eisenbach, T. M., Kovner, A., and Lee, M. J. (2022), "Cyber risk and the US financial system: A pre-mortem analysis, *Journal of Financial Economics,* Vol. 145 No. 3, pp. 802-826.

Fang, X., Pittman, J., & Zhao, Y. (2021). The importance of director external social networks to stock price crash risk. *Contemporary Accounting Research*, *38*(2), 903-941.

Ferracone. (2019). Good governance: Do boards need cyber security experts?. *Forbes*. Available at: https://www.forbes.com/sites/robinferracone/2019/07/09/good-governance-do-boards-need-cyber-security-experts/?sh=15d506f21859 (Accessed September 10, 2022).

Florackis, C., Louca, C., Michaely, R., & Weber, M. (2023). Cybersecurity risk. *The Review of Financial Studies*, *36* (1), 351-407.

Frank, M. L., Grenier, J. H., & Pyzoha, J. S. (2021). Board liability for cyberattacks: The effects of a prior attack and implementing the AICPA's cybersecurity framework. *Journal of Accounting and Public Policy*, 106860.

Gartner. (2021). Forecast: Information security and risk management, worldwide, 2019-2025, 1Q21 update. Available at: https://www.gartner.com/en/documents/3999995 (Accessed October 11, 2022)

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & 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.

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2015). Increasing cybersecurity investments in private sector firms. *Journal of Cybersecurity, 1*(1), 3-17.

Gwebu, K. L., Wang, J., & Wang, L. (2018). The role of corporate reputation and crisis response strategies in data breach management. *Journal of Management Information Systems*, *35*(2), 683-714.

Hadden, L. B., Hermanson, D. R., & DeZoort, F. T. (2003). Audit committees' oversight of information technology risk. *Review of Business Information Systems (RBIS)*, *7*(4), 1-12.

Haislip, J., K. Kolev, R. Pinskerf, and T. Steffen. 2019. The economic cost of cybersecurity breaches: A broad-based analysis. Working paper, Texas Tech University, Baruch College, Florida Atlantic University, and Yale University.

Haislip, J., Lim, J. H., & Pinsker, R. (2021). The impact of executives' it expertise on reported data security breaches. *Information Systems Research, 32*(2), 318-334.

Higgs, J. L., Pinsker, R. E., Smith, T. J., & Young, G. R. (2016). The relationship between board-level technology committees and reported security breaches. *Journal of Information Systems*, *30*(3), 79-98.

Hsu, C., & Wang, T. (2014). Exploring the association between board structure and information security breaches. *Asia Pacific Journal of Information Systems*, *24*(4), 531-557.

Huang, H. H., & Wang, C. (2021). Do banks price firms' data breaches?. *The Accounting Review*, 96(3), 261-286.

Huang, H., Lobo, G. J., & Zhou, J. (2009). Determinants and accounting consequences of forming a governance committee: Evidence from the United States. *Corporate Governance: An International Review*, *17*(6), 710-727.

IBM. (2020). Cost of a data breach report 2020. Available at: https://www.ibm.com/downloads/cas/RZAX14GX (Accessed April 12, 2021).

IBM. (2022). Cost of a data breach report 2022. Available at: https://www.ibm.com/security/data-breach (Accessed August 22, 2021)

Institute of Internal Auditors (IIA). (2016). Assessing cybersecurity risk: Roles of the three lines of defense. Available at : https://na.theiia.org/standards-guidance/recommended-guidance/practice-guides/Pages/GTAG-Assessing-Cybersecurity-The-Three-Lines-Model.aspx

ISO. (2013). Information security management. Available at: https://www.iso.org/isoiec-27001-information-security.html (Accessed June 2, 2021).

Jaeger, J. (2012). When to go public about a data breach. *Compliance Week*, 9(103), 38-39,66

Jewer, J., & McKay, K. N. (2012). Antecedents and consequences of board IT governance: Institutional and strategic choice perspectives. *Journal of the Association for Information Systems*, *13*(7), 1.

Jiang, W., Legoria, J., Reichelt, K., & Walton, S. (2021). Firm use of cybersecurity risk disclosure. *Journal of Information Systems, 36*(1), 151-180.

Kamiya, S., Kang, J. K., Kim, J., Milidonis, A., & Stulz, R. M. (2021). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics*, *139*(3), 719-749.

Klein, A., Manini, R., & Shi, Y. (2022). Across the pond: How US firms' boards of directors adapted to the passage of the General Data Protection Regulation. *Contemporary Accounting Research, 39*(1), 199-233.

Klemash S. W., Smith J. C., & Seets C. W. (2020). What companies are disclosing about cybersecurity risk and oversight. *Harvard Law School Forum on Corporate Governance*. Available at: https://corpgov.law.harvard.edu/2020/08/25/what-companies-are-disclosing-about-cybersecurity-risk-and-oversight/ (Accessed 30 April 2021)

Klemash, S. W., Cordero, P., & Seets, C. W. (2019). Cyber risk board oversight. *Harvard Law School Forum on Corporate Governance.* Available at https://corpgov.law.harvard.edu/ (Accessed 11 July 2021).

KPMG. (2016). Cyber security is a critical audit committee issue. Audit point of view. Available at https://assets.kpmg/content/dam/kpmg/ca/pdf/2016/08/ca-cyber-security-is-a-critical-audit.pdf

Landefeld, S. M., Mejia, L. R., & Handy, A. C. (2015). Board tools for oversight of cybersecurity risk. *The Corporate Governance Advisor*, *23*(3), 1-9.

Landefeld, S., Mejia, L., Handy, A., & Hinnen, T. (2017). Is that a target on your back?': Board cybersecurity oversight duty after the Target settlement. *The Corporate Governance Advisor, 25*(6), 1-9.

Lankton, N., Price, J. B., & Karim, M. (2021). Cybersecurity breaches and the role of information technology governance in audit committee charters. *Journal of Information Systems*, *35*(1), 101-119.

Larcker, D. F., So, E. C., & Wang, C. C. (2013). Boardroom centrality and firm performance. *Journal of Accounting and Economics*, *55*(2-3), 225-250.

Lawrence, A., Minutti-Meza, M., & Vyas, D. (2018). Is operational control risk informative of financial reporting deficiencies?. *Auditing: A Journal of Practice & Theory, 37*(1), 139-165.

Lending, C., Minnick, K., & Schorno, P. J. (2018). Corporate governance, social responsibility, and data breaches. *The Financial Review*, *53*(2), 413-455.

Li, H., No, W. G., & Boritz, J. E. (2020). Are external auditors concerned about cyber incidents? Evidence from audit fees. *Auditing: A Journal of Practice & Theory*, *39*(1), 151-171.

Lin, Z., Sapp, T. R., Ulmer, J. R., & Parsa, R. (2020). Insider trading ahead of cyber breach announcements. *Journal of Financial Markets, 50*, 100527.

Loop, P. (2016). Cybersecurity and the board: 8 Issues keeping directors up at night. *Wall Street Journal*. https://sponsoredcontent.wsj.com/pwc/broader-perspectives/cybersecurity-and-the-board-8-issues-keeping-directors-up-at-night/.

Lowry, M., Vance, A., & Vance, M. D. (2021). Inexpert supervision: Field evidence on boards' oversight of cybersecurity. Available at SSRN 4002794.
Maurer, C., Kim, K., Kim, D., & Kappelman, L. A. (2021). Cybersecurity: Is it worse than we think?. *Communications of the ACM*, *64*(2), 28-30.
McGrath, V., Sheedy, E. A., & Yu, F. (2021). Governance of cyber security: State of play. *Available at SSRN 3971177*.
Moore, T., Dynes, S., & Chang, F. R. (2015). Identifying how firms manage cybersecurity investment. *Southern Methodist University. Available at: https://tylermoore.ens.utulsa.edu/ciso15ibm.pdf*
National Institute of Standards and Technology (NIST). (2018). Framework for improving critical infrastructure cybersecurity. Available at: https://nvlpubs.nist.Gov/nistpubs/ CSWP/NIST.CSWP. 04162018 .pdf
New York Stock Exchange (NYSE) (2021). NYSE Listed Company Manual Section 303A. Section 303A.07 – Audit Committee Additional Requirements. Available at: https://www.nyse.com/publicdocs/nyse /regulation/nyse/FAQ_NYSE_Listed_Company_Manual_Section_303A_7_28_2021.pdf
Nolan, R., & McFarlan, F. W. (2005). Information technology and the board of directors. *Harvard Business Review*, *83*(10), 96.
Nordlund, J. (2019). The disclosure of cybersecurity risk. *Available at SSRN 3077632.*
Piccotti, L. R., & Wang, H. E. (2021). Informed trading in options markets surrounding data breaches. *Available at SSRN 3478263*.
Price, J. B., & Lankton, N. (2018). A framework and guidelines for assessing and developing board-level information technology committee charters. *Journal of Information Systems*, *32*(1), 109-129.
Public Company Accounting Oversight Board (PCAOB). (2018). Strategic plan 2018–2022. Available at: https://pcaob-assets.azureedge.net/pcaob-dev/docs/default-source/about/ administration/documents/strategic_plans/pcaob-2018-2022-strategic-plan.pdf?sfvrsn =d7 4236b3_0 (Accessed August 20, 2021).
PwC. (2018). The evolving boardroom signs of change: 2018 Annual corporate directors survey. Available at: https://www.corporatecomplianceinsights.com/wp-content/uploads/2018/ 10/PwC-2018-ACDS.pdf
Radu, C., & Smaili, N. (2021). Board gender diversity and corporate response to cyber risk: Evidence from cybersecurity related disclosure. *Journal of Business Ethics*, *177*, 351–374.
Rajgopal, S., & Srinivasan, S. (2016, October 4). Why the market yawned when yahoo was hacked. *Wall Street Journal.* Retrieved May 2, 2021, from https://www.wsj.com/articles/why-the-market-yawned-when-yahoo-was-hacked-1475537076
Richardson, V. J., Smith, R. E., & 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.
Romanosky, S. (2016). Examining the costs and causes of cyber incidents. *Journal of Cybersecurity*, *2*(2), 121-135.
Rosati, P., Gogolin, F., & Lynn, T. (2019). Audit firm assessments of cyber-security risk: Evidence from audit fees and SEC comment letters. *The International Journal of Accounting*, *54*(03), 1950013.
Rothrock, R. A., Kaplan, J., & Van Der Oord, F. (2018). The board's role in managing cybersecurity risks. *MIT Sloan Management Review*, *59*(2), 12-15.

Securities and Exchange Commission (SEC). (2005). Securities and Exchange Commission final rule, release no.33–8591(fr-75). Available at: http://www.sec.gov/rules/final/33-8591.pdf.
Securities and Exchange Commission (SEC). (2011). Cf disclosure guidance: Topic no. 2. Available at: Https://www.Sec.Gov/divisions/corpfin/guidance/cfguidance-topic2.Htm.
Securities and Exchange Commission (SEC). (2018). Commission statement and guidance on public company cybersecurity disclosures (February 26). Available at https://www.sec.gov/rules/interp/2018/33-10459.pdf.
Securities and Exchange Commission (SEC). (2022). Proposed rule: Cybersecurity risk management, strategy, governance, and incident disclosure. Available at: https://www.sec.gov/rules/proposed/2022/33-11038.pdf.
Security and Exchange Commission (SEC). (2009). Proxy disclosure enhancements. A*vailable at* http://www.sec.gov/rules/final/2009/33-9089.pdf
Security and Exchange Commission (SEC). (2021). SEC announces three actions charging deficient cybersecurity procedures. In 2021-169. Washington, D.C.: Securities and Exchange Commission. Available at: https://www.sec.gov/news/press-release/2021-169
Sen, R., & Borle, S. (2015). Estimating the contextual risk of data breach: An empirical approach. *Journal of Management Information Systems*, *32*(2), 314-341.
Slapničar, S., Axelsen, M., Bongiovanni, I., & Stockdale, D. (2022). A pathway model to five lines of accountability in cybersecurity governance. *Available at SSRN 4176559*.
Smith, T. J., Higgs, J. L., & Pinsker, R. E. (2019). Do auditors price breach risk in their audit fees?. *Journal of Information Systems*, *33*(2), 177-204.
Smith, T., Tadesse, A. F., & Vincent, N. E. (2021). The impact of CIO characteristics on data breaches. *International Journal of Accounting Information Systems, 43,* 100532.
Sonnemaker, T. (2019, March 9). *Facing Inevitable Data Breaches and New Privacy Laws, Companies Shift Focus to Response*. Medill Reports Chicago. Available at: https://news.medill.northwestern.edu/chicago/facing-inevitable-data-breaches-and-new-privacylaws-companies-shift-focus-to-response/
SpencerStuart. (2016). Spencer Stuart board index. Available at: https://www.spencerstuart.com/~/media/pdf% 20 files/research%20and%20insight%20pdfs/spencer-stuart-us-board-index-2016.pdf. (Accessed 23 July 2021)
Sumner, P., Day J., & Mahoney M. (2020). Cybersecurity: An evolving governance challenge. *Harvard Law School Forum on Corporate Governance*, Available at: https://corpgov.law.harvard.edu/2020/03/15/cybersecurity-an-evolving-governance-challenge/ (Accessed 11 June 2021)
Trautman, L. J., Butler, S., Chang, F. R., Hooper, M., McCray, R., & Simmons, R. (2022). Corporate directors: Who they are, what they do, cyber risk and other challenges. *Buffalo Law Review*, *70,* 459.
Tsukayama, H. (2017). Why it can take so long for companies to reveal their data breaches. *The Washington Post*. Available at: https://www.washingtonpost.com/news/the-switch/wp/2017/09/08/why-it-can-take-so-long-for-companies-to-reveal-their-data-breaches/ (Accessed June 3, 2021).
Turel, O., & Bart, C. (2014). Board-level IT governance and organizational performance. *European Journal of Information Systems*, *23*(2), 223-239.
US Congress. (2021). S.592 - Cybersecurity Disclosure Act of 2019. Available at: https://www.congress.gov/bill/116th-congress/senate-bill/592?q=%7B%22search%22%3

A%5B%22%5C%22Cybersecurity+Disclosure%5C%22+Act+of+2019%22%5D%7D&s=3&r=4

Wang, T., & Hsu, C. (2013). Board composition and operational risk events of financial institutions. *Journal of Banking & Finance*, *37*(6), 2042-2051.

Yen, J. C., Lim, J. H., Wang, T., & Hsu, C. (2018). The impact of audit firms' characteristics on audit fees following information security breaches. *Journal of Accounting and Public Policy*, *37*(6), 489-507.

Yew, S. W., T. I. Houw, T. T. Gan, D. Lim, & K. Leong. (2015). Cybersecurity: The changing role of audit committee and internal audit. Available at: https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sea-risk-cyber-security-changing-role-in-audit-noexp.pdf

Zafar, H., Ko, M. S., & Osei-Bryson, K. M. (2016). The value of the CIO in the top management team on performance in the case of information security breaches. *Information Systems Frontiers, 18*(6), 1205-1215.

**Figure 1 Cybersecurity Risk Oversight Assignment Over the Years**

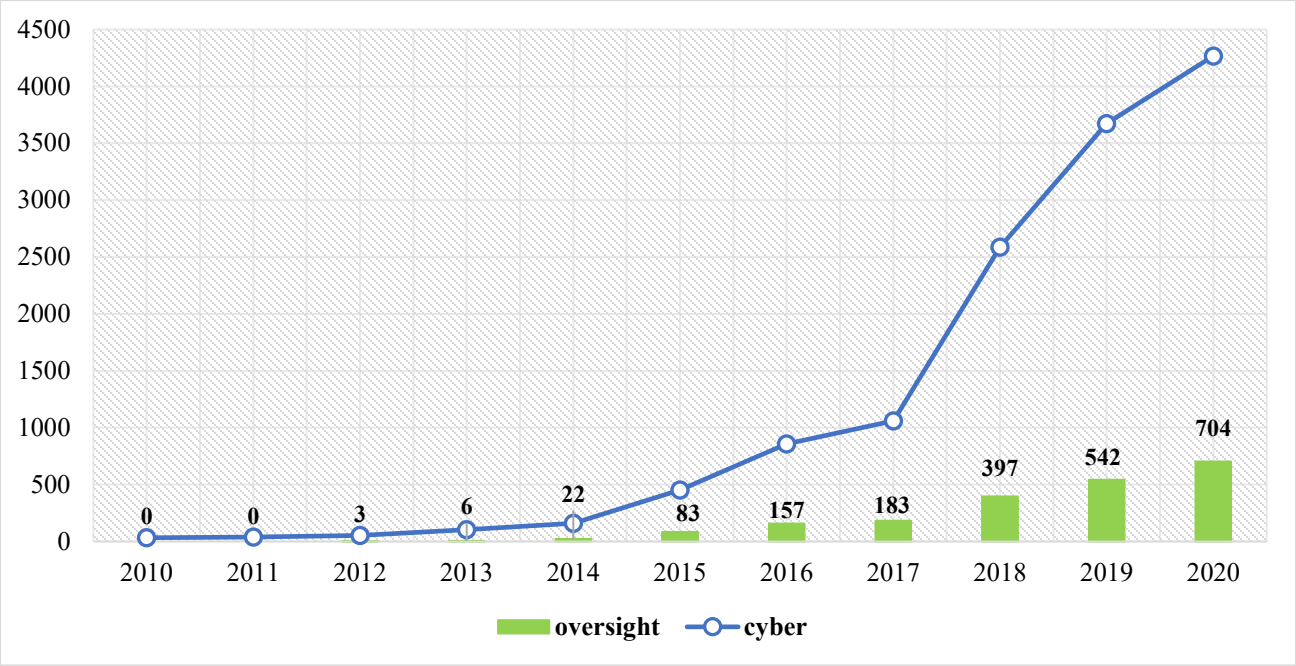


Figure 1 shows distribution of observations with explicit assignment of cybersecurity risk oversight responsibility in proxy statements over the years 2010-2020. The line chart displays distribution of the term "cyber" in proxy statements over the same period.

TABLE 1 **Sample Selection**

**Data Breach Sample**

| **Panel A: Cybersecurity Breach Incidents Sample** | **No. of Events** | **No. of Firms** |
|---|---|---|
| Total number of cyber incidents from 2010 to 2020 (Advisen) | 146,651 | 54,266 |
| Less: Government, not for profit, and private organizations | (107,373) | (45,578) |
| Less: Non-U.S. publicly listed companies | (4,537) | (2,227) |
| Less: Observations with missing CIK | (20,809) | (4,646) |
| **Total number of cyber events of publicly listed U.S. companies** | **13,932** | **1,815** |

**Main Sample**

| **Panel B: Proxy Statement Sample Selection** | **No. of Obs.** | **No. of Firms** |
|---|---|---|
| Firm proxy statements (DEF 14A) filings from 2010- 2020 | 9,268 | 950 |
| Less: Missing data to calculate determinants and control variables (BoardEx and Compustat) | (1,971) | (47) |
| **Total observations in main determinants sample** | **7,297** | **903** |

| **Panel C: Sample Distribution by Fama-French 12 Industries** | **No. of Obs.** | **No. of Firms** |
|---|---|---|
| Consumer Nondurables | 306 | 35 |
| Consumer Durables | 120 | 14 |
| Manufacturing | 532 | 63 |
| Energy, Oil, and Gas | 145 | 19 |
| Chemicals and Allied Products | 132 | 15 |
| Computers, Software, and Electronic Equipment | 1,265 | 180 |
| Telephone and Television Transmission | 232 | 29 |
| Utilities | 222 | 25 |
| Wholesale, Retail, and Some Services | 1,013 | 125 |
| Healthcare, Medical Equipment, and Drugs | 570 | 76 |
| Finance | 1,641 | 189 |
| Other | 1,119 | 133 |
| **Total** | **7,297** | **903** |

Table 1 presents study sample selection. Panel A provides cybersecurity incidents sample construction. Panel B reports the study's main sample construction. Panels C provides distributions of the main sample observations by Fama-French 12 industries.

TABLE 2

**Descriptive Statistics**

**Panel A: Descriptive Statistics For Oversight Sample (n = 7,297)**

| Variable | Mean | Std. Dev. | 25% | Median | 75% |
|---|---|---|---|---|---|
| Test Variable | | | | | |
| **Oversight Level 1** | | | | | |
| *OVERSIGHT* $_t$ (binary) | 0.29 | 0.45 | 0.00 | 0.00 | 1.00 |
| Dependent Variable | | | | | |
| *BOARD_SIZE* $_{t-1}$ | 9.72 | 2.55 | 8.00 | 10.00 | 11.00 |
| *COMPETENCY* $_{t-1}$ | 0.01 | 0.03 | 0.00 | 0.00 | 0.00 |
| *NETWORK_SIZE* $_{t-1}$ | 10.00 | 1.08 | 9.31 | 9.94 | 10.69 |
| *EQUITY_HOLDING* $_{t-1}$ | 4.52 | 5.87 | 0.00 | 0.00 | 11.17 |
| *GENDER_DIVERSITY* $_{t-1}$ | 0.83 | 0.11 | 0.75 | 0.83 | 0.90 |
| Control Variables | | | | | |
| *SIZE* $_{t-1}$ | 8.32 | 2.13 | 6.91 | 8.30 | 9.75 |
| *ROA* $_{t-1}$ | 2.29 | 16.58 | 0.79 | 3.49 | 7.56 |
| *LOSS* $_{t-1}$ (binary) | 0.18 | 0.39 | 0.00 | 0.00 | 0.00 |
| *LEVERAGE* $_{t-1}$ | 0.23 | 0.25 | 0.04 | 0.19 | 0.34 |
| *SALES_GROWTH* $_{t-1}$ | 11.08 | 78.76 | 0.00 | 3.37 | 11.87 |
| *Z_SCORE* $_{t-1}$ | 0.92 | 4.10 | 0.23 | 1.11 | 2.17 |
| *FIRM_AGE* $_{t-1}$ | 29.71 | 18.94 | 16.00 | 23.00 | 44.00 |
| *ACQUISITION* $_{t-1}$ (binary) | 0.10 | 0.30 | 0.00 | 0.00 | 0.00 |
| *FOREIGN* $_{t-1}$ (binary) | 0.47 | 0.50 | 0.00 | 0.00 | 1.00 |
| *SEGMENTS_B* $_{t-1}$ | 0.45 | 0.65 | 0.00 | 0.00 | 0.69 |
| *SEGMENTS_G* $_{t-1}$ | 0.40 | 0.64 | 0.00 | 0.00 | 0.69 |
| *RESTRUCTURE* $_{t-1}$ (binary) | 0.38 | 0.48 | 0.00 | 0.00 | 1.00 |
| *NYSE* $_{t-1}$ (binary) | 0.54 | 0.50 | 0.00 | 1.00 | 1.00 |
| *CYBER_RISK* $_{t-1}$ (binary) | 0.71 | 0.45 | 0.00 | 1.00 | 1.00 |

**Panel B: Other Descriptive Statistics**

| Variable | Mean | Std. Dev. | 25% | Median | 75% |
|---|---|---|---|---|---|
| Test Variable | | | | | |
| **Oversight Level 2 (n = 2,097)** | | | | | |
| *OVERSIGHT* $_t$ (binary) | 0.16 | 0.37 | 0.00 | 0.00 | 0.00 |
| **Oversight Level 3 (n = 1,751)** | | | | | |
| *OVERSIGHT* $_t$ (binary) | 0.58 | 0.49 | 0.00 | 1.00 | 1.00 |

Table 2 presents summary statistics for cybersecurity oversight sample for the period 2010 to 2020. Panel (A) provides descriptive statistics for cybersecurity oversight level 1 (7,297 observations), where *OVERSIGHT* $_t$ is an indicator variable equal to one for firm *i* with an explicit cybersecurity risk oversight assignment in year *t* and zero otherwise, *BOARD_SIZE* $_{t-1}$ is number of board members, *NETWORK_SIZE* $_{t-1}$ is a board network size, *GENDER_DIVERSITY* $_{t-1}$ is percentage of female directors, *COMPETENCY* $_{t-1}$ is percentage of directors' cybersecurity/IT competency and experience, *EQUITY_HOLDING* $_{t-1}$ is board equity holding, *SIZE* is natural log of firms' total assets, *ROA* $_{t-1}$ is net income scaled by total assets, *LOSS* $_{t-1}$ is an indicator variable that takes the value of one if net income before extraordinary items is negative, zero otherwise *LEVERAGE* $_{t-1}$ is long-term debt scaled by total assets, *Z_SCORE* $_{t-1}$ is Modified Altman (1968) Z-score, *SALES_GROWTH* $_{t-1}$ is a firms' sales growth, *FIRM_AGE* $_{t-1}$ is the firm age, *ACQUISITION* $_{t-1}$ is an indicator variable for firms with acquisitions, *FOREIGN* is an indicator variable for firms with

foreign operations, $SEGMENTS\_B_{t-1}$ is firms' number of business segments, $SEGMENTS\_G_{t-1}$ is firms' number of geographic segments, $RESTRUCTURE_{t-1}$ is an indicator variable for firms with restructuring, $NYSE_{t-1}$ is an indicator variable for firm's listed on the New York Stock Exchange, and $CYBER\_RISK_{t-1}$ is an indicator variable for firm's that belong to high cyber risk industries.

Panel (B) presents descriptive statistics for cybersecurity oversight level 2 (2,097 observations), where $OVERSIGHT_t$ is defined one for firm *i* that assigns cybersecurity risk oversight in year *t* to the full board and zero if assigned to a board-level committee(s); and Level 3 (1,757 observations), where $OVERSIGHT_t$ is defined one for firm *i* that assigns cybersecurity risk oversight in year *t* to the audit committee and zero if assigned to a non-audit board-level committee(s).

TABLE 3 **Pearson Correlations for Oversight Sample**

**Sample n = 7,297**

| | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **1** | *OVERSIGHT* $_{t}$ | | | | | | | | | | | | | | | | | | | |
| **2** | *BOARD_SIZE* $_{t-1}$ | **0.14** | | | | | | | | | | | | | | | | | | |
| **3** | *COMPETENCY* $_{t-1}$ | **0.07** | 0.02 | | | | | | | | | | | | | | | | | |
| **4** | *NETWORK_SIZE* $_{t-1}$ | **0.22** | **0.60** | **0.08** | | | | | | | | | | | | | | | | |
| **5** | *EQUITY_HOLDING* $_{t-1}$ | **0.17** | **0.49** | **0.10** | **0.71** | | | | | | | | | | | | | | | |
| **6** | *GENDER_DIVERSITY* $_{t-1}$ | **-0.26** | **-0.24** | **-0.05** | **-0.32** | **-0.26** | | | | | | | | | | | | | | |
| **7** | *SIZE* $_{t-1}$ | **0.23** | **0.65** | **0.04** | **0.68** | **0.67** | **-0.32** | | | | | | | | | | | | | |
| **8** | *ROA* $_{t-1}$ | **0.05** | **0.14** | **-0.01** | **0.11** | **0.19** | **-0.10** | **0.24** | | | | | | | | | | | | |
| **9** | *LOSS* $_{t-1}$ | **-0.04** | **-0.24** | **0.03** | **-0.12** | **-0.24** | **0.13** | **-0.33** | **-0.53** | | | | | | | | | | | |
| **10** | *LEVERAGE* $_{t-1}$ | **0.11** | 0.00 | **-0.03** | 0.05 | **0.02** | **-0.04** | **0.07** | 0.01 | **0.05** | | | | | | | | | | |
| **11** | *SALES_GROWTH* $_{t-1}$ | **-0.02** | **-0.06** | 0.00 | **-0.04** | **-0.05** | **0.06** | **-0.09** | 0.01 | **0.07** | -0.01 | | | | | | | | | |
| **12** | *Z_SCORE* $_{t-1}$ | **0.02** | **0.10** | -0.02 | **0.05** | **0.09** | **-0.08** | **0.14** | **0.41** | **-0.29** | **-0.04** | **-0.02** | | | | | | | | |
| **13** | *FIRM_AGE* $_{t-1}$ | **0.14** | **0.40** | 0.01 | **0.41** | **0.43** | **-0.26** | **0.45** | **0.16** | **-0.19** | **0.03** | **-0.09** | **0.11** | | | | | | | |
| **14** | *ACQUISITION* $_{t-1}$ | **-0.03** | **-0.07** | -0.01 | **-0.04** | **-0.05** | **0.07** | **-0.05** | 0.00 | **0.02** | **0.04** | **0.07** | 0.00 | **-0.06** | | | | | | |
| **15** | *FOREIGN* $_{t-1}$ | **0.07** | **0.09** | 0.01 | **0.28** | **0.23** | **-0.12** | **0.13** | **0.18** | **-0.15** | **0.04** | **-0.03** | **0.11** | **0.15** | **0.06** | | | | | |
| **16** | *SEGMENTS_B* $_{t-1}$ | **0.37** | -0.01 | 0.02 | **0.08** | **0.04** | **-0.16** | **0.04** | -0.01 | **0.05** | **0.09** | -0.01 | 0.01 | **0.10** | **0.03** | **0.07** | | | | |
| **17** | *SEGMENTS_G* $_{t-1}$ | **0.33** | **-0.03** | **0.06** | **0.09** | **0.04** | **-0.13** | **0.00** | **-0.02** | **0.09** | **0.07** | 0.01 | -0.01 | **0.07** | **0.02** | **0.21** | **0.73** | | | |
| **18** | *RESTRUCTURE* $_{t-1}$ | **0.10** | **0.11** | -0.01 | **0.23** | **0.10** | **-0.14** | **0.08** | 0.02 | **0.05** | **0.08** | **-0.06** | **0.02** | **0.16** | **0.04** | **0.29** | **0.12** | **0.17** | | |
| **19** | *NYSE* $_{t-1}$ | **0.11** | **0.27** | **0.02** | **0.29** | **0.26** | **-0.17** | **0.41** | **0.14** | **-0.16** | **0.13** | **-0.06** | **0.13** | **0.32** | **-0.04** | **0.12** | **0.06** | 0.01 | **0.08** | |
| **20** | *CYBER_RISK* $_{t-1}$ | **-0.02** | **0.06** | **0.04** | **0.04** | **0.04** | **-0.04** | **0.05** | **-0.08** | **0.05** | **-0.20** | **0.02** | **-0.09** | 0.00 | -0.01 | **0.04** | -0.02 | **0.07** | **0.05** | **-0.08** |

Table 3 reports Pearson correlation coefficients for cybersecurity risk oversight (level 1) sample. Appendix B contains the definitions of the variables. Values in bold indicate statistical significance at 1 percent or better.

TABLE 4 **Exploratory Analysis of Cybersecurity Risk Oversight**

**Panel A: Cybersecurity Risk Oversight Assignment in Proxy Statements**

| **Oversight** | **Frequency** | **Percent** |
|---|---|---|
| No Cybersecurity Risk Oversight Specified | 5,200 | 71% |
| Cybersecurity Risk Oversight | 2,097 | 29% |
| **Total** | **7,297** | **100%** |

| **Classification of Cybersecurity Risk Oversight Location** | **Frequency** | **Percent** |
|---|---|---|
| Audit Committee (AC) | 1,198 | 57% |
| Compliance Committee (CC) | 19 | 1% |
| Cybersecurity Committee (CSC) | 48 | 2% |
| Finance Committee (FC) | 34 | 2% |
| Full Board (FB) | 346 | 17% |
| Joint Committee (JC) | 66 | 3% |
| Nominating and Governance Committee (NGC) | 31 | 1% |
| Risk Committee (RC) | 226 | 11% |
| Technology Committee (TC) | 102 | 5% |
| Other (OTH) | 27 | 1% |
| **Total** | **2,097** | **100%** |

**Panel B: Cybersecurity Risk Oversight Preference by Fama-French 12 Industries**

| **Fama-French 12 Industries** | **AC** | **CC** | **CSC** | **FC** | **FB** | **JC** | **NGC** | **OTH** | **RC** | **TC** | **Total** |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Consumer Nondurables | 36 | 1 | 3 | | 13 | | | | 1 | | 54 |
| Consumer Durables | 25 | | 3 | | 5 | | 1 | | 1 | 6 | 41 |
| Manufacturing | 102 | | 2 | 5 | 31 | 3 | 3 | 1 | | 5 | 152 |
| Energy, Oil, and Gas | 35 | | | | 10 | | | 1 | | | 46 |
| Chemicals and Allied Products | 31 | | | | 5 | | | | 1 | | 37 |
| Computers, Software, and Electronic Equipment | 330 | 3 | 18 | 4 | 93 | 10 | 4 | 9 | 18 | 13 | 502 |
| Telephone and Television Transmission | 39 | | | | 11 | 3 | 5 | | 6 | | 64 |
| Utilities | 36 | | 6 | 12 | 13 | | | 9 | 5 | 3 | 84 |
| Wholesale, Retail, and Some Services | 180 | 4 | 6 | 7 | 51 | 2 | 2 | | 10 | 6 | 268 |
| Healthcare, Medical Equipment, and Drugs | 73 | 6 | 1 | | 19 | 2 | 2 | | 1 | 2 | 106 |
| Finance | 155 | 4 | 6 | 6 | 49 | 34 | 1 | 1 | 165 | 49 | 470 |
| Other | 156 | 1 | 3 | | 46 | 12 | 13 | 6 | 18 | 18 | 273 |
| **Total** | **1,198** | **19** | **48** | **34** | **346** | **66** | **31** | **27** | **226** | **102** | **2,097** |

Table 4 provides analysis of cybersecurity risk oversight assignment location. Panel A presents the frequency (percentage) of ten categories of oversight assignment. Panel B reports distribution of ten classification of oversight location: full board (FB), audit committee (AC), finance committee (FC), technology committee (TC), compliance committee (CC), risk committee (RC), joint committee (JC), cybersecurity committee (CSC), nominating and governance committee (NGC), and "other" committee (OTH) by Fama-French 12 industries.

TABLE 5 **Level 1 Analysis: Disclosure of Cybersecurity Risk Oversight Responsibility Assignment**

| | **Dependent Variable: $OVERSIGHT_t$** | | |
|---|---|---|---|
| **Independent Variables** | **No Controls or Fixed Effects (1)** | **No Controls (2)** | **Full Model (3)** |
| Test Variables | | | |
| *BOARD_SIZE* $_{t-1}$ | 0.006 | 0.027 | -0.020 |
| | (0.449) | (1.517) | (-1.010) |
| *COMPETENCY* $_{t-1}$ | 3.292*** | 1.887** | 2.687*** |
| | (4.241) | (2.007) | (2.792) |
| *NETWORK_SIZE* $_{t-1}$ | 0.354*** | 0.563*** | 0.411*** |
| | (8.467) | (10.196) | (6.899) |
| *EQUITY_HOLDING* $_{t-1}$ | -0.003 | 0.010 | -0.016* |
| | (-0.422) | (1.196) | (-1.726) |
| *GENDER_DIVERSITY* $_{t-1}$ | -4.421*** | -1.545*** | -1.048*** |
| | (-16.900) | (-4.698) | (-3.086) |
| Control Variables | | | |
| *SIZE* $_{t-1}$ | | | 0.198*** |
| | | | (6.703) |
| *ROA* $_{t-1}$ | | | 0.006 |
| | | | (1.635) |
| *LOSS* $_{t-1}$ | | | -0.024 |
| | | | (-0.203) |
| *LEVERAGE* $_{t-1}$ | | | 0.513*** |
| | | | (3.438) |
| *SALES_GROWTH* $_{t-1}$ | | | 0.000 |
| | | | (-0.015) |
| *Z_SCORE* $_{t-1}$ | | | 0.005 |
| | | | (0.372) |
| *FIRM_AGE* $_{t-1}$ | | | -0.001 |
| | | | (-0.248) |
| *ACQUISITION* $_{t-1}$ | | | -0.238** |
| | | | (-2.009) |
| *FOREIGN* $_{t-1}$ | | | 0.149* |
| | | | (1.841) |
| *SEGMENTS_B* $_{t-1}$ | | | 0.046 |
| | | | (0.639) |
| *SEGMENTS_G* $_{t-1}$ | | | 0.101 |
| | | | (1.406) |
| *RESTRUCTURE* $_{t-1}$ | | | 0.223*** |
| | | | (2.932) |
| *NYSE* $_{t-1}$ | | | 0.157** |
| | | | (2.036) |
| *CYBER_RISK* $_{t-1}$ | | | -0.036 |
| | | | (-0.392) |
| Year Fixed Effects | No | Yes | Yes |
| Industry Fixed Effects | No | Yes | Yes |
| Observations | 7297 | 7297 | 7297 |

| | | | |
|---|---|---|---|
| Pseudo $R^2$ | 0.091 | 0.362 | 0.373 |
| Area Under ROC | 0.692 | 0.887 | 0.893 |

Table 5 shows governance determinants of cybersecurity risk oversight assignment. The dependent variable in the regression is $OVERSIGHT_t$, defined as one for firm $i$ with an explicit cybersecurity risk oversight assignment in year $t$ and zero otherwise. Column (1) presents regression results without controls and fixed effects, Column (2) presents results with fixed effects, and Column (3) reports results with controls and fixed effects (i.e., full model).

All variables are defined in detail in Appendix B.

The regression includes an intercept but is not tabulated for brevity. The *t*-statistics are in parentheses and ***, **, and * indicate significance at the 0.01, 0.05, and 0.10 levels, respectively.

TABLE 6 **Level 2 Analysis: Disclosure of Cybersecurity Risk Oversight Responsibility Assignment to Full Board or Board-Level Committee(s)**

| | Dependent Variable: $OVERSIGHT_t$ | | |
|---|---|---|---|
| **Independent Variables** | **No Controls or Fixed Effects (1)** | **No Controls (2)** | **Full Model (3)** |
| Test Variables | | | |
| *BOARD_SIZE* $_{t-1}$ | -0.169*** | -0.153*** | -0.086** |
| | (-4.913) | (-4.230) | (-2.155) |
| *COMPETENCY* $_{t-1}$ | -1.193 | -1.048 | -0.939 |
| | (-0.728) | (-0.636) | (-0.570) |
| *NETWORK_SIZE* $_{t-1}$ | 0.033 | -0.015 | 0.020 |
| | (0.329) | (-0.139) | (0.169) |
| *EQUITY_HOLDING* $_{t-1}$ | -0.036** | -0.035** | -0.009 |
| | (-2.395) | (-2.226) | (-0.519) |
| *GENDER_DIVERSITY* $_{t-1}$ | 1.004* | 0.736 | 0.740 |
| | (1.721) | (1.206) | (1.149) |
| Control Variables | | | |
| *SIZE* $_{t-1}$ | | | -0.281*** |
| | | | (-4.912) |
| *ROA* $_{t-1}$ | | | 0.012* |
| | | | (1.705) |
| *LOSS* $_{t-1}$ | | | 0.423** |
| | | | (2.045) |
| *LEVERAGE* $_{t-1}$ | | | -0.335 |
| | | | (-1.264) |
| *SALES_GROWTH* $_{t-1}$ | | | 0.001 |
| | | | (0.663) |
| *Z_SCORE* $_{t-1}$ | | | -0.018 |
| | | | (-0.826) |
| *FIRM_AGE* $_{t-1}$ | | | 0.018*** |
| | | | (4.425) |
| *ACQUISITION* $_{t-1}$ | | | 0.392* |
| | | | (1.935) |
| *FOREIGN* $_{t-1}$ | | | 0.233 |
| | | | (1.547) |
| *SEGMENTS_B* $_{t-1}$ | | | 0.333*** |
| | | | (2.699) |
| *SEGMENTS_G* $_{t-1}$ | | | -0.322** |
| | | | (-2.562) |
| *RESTRUCTURE* $_{t-1}$ | | | -0.077 |
| | | | (-0.560) |
| *NYSE* $_{t-1}$ | | | -0.233* |
| | | | (-1.652) |
| *CYBER_RISK* $_{t-1}$ | | | 0.382** |
| | | | (2.308) |
| Year Fixed Effects | No | Yes | Yes |
| Industry Fixed Effects | No | Yes | Yes |
| Observations | 2097 | 2097 | 2097 |

| | | | |
|---|---|---|---|
| Pseudo $R^2$ | 0.038 | 0.046 | 0.082 |
| Area Under ROC | 0.648 | 0.653 | 0.699 |

Table 6 shows governance determinants of the full board versus board-level committee cybersecurity risk oversight assignment. The dependent variable in the regression is $OVERSIGHT_t$, defined as one for firm *i* that assigns cybersecurity risk oversight in year *t* to the full board and zero if assigned to a board-level committee(s). Column (1) provides regression results without controls and fixed effects, Column (2) presents results with fixed effects, and Column (3) reports results for the full model. The regression includes an intercept but is not tabulated for brevity.

Appendix B contains definitions of variables.

The *t*-statistics are in parentheses and ***, **, and * indicate significance at the 0.01, 0.05, and 0.10 levels, respectively.

TABLE 7 **Level 3 Analysis: Disclosure of Cybersecurity Risk Oversight Responsibility Assignment to the Audit Committee or Non-Audit Board-Level Committee(s)**

| | **Dependent Variable: *OVERSIGHT* $_t$** | | |
|---|---|---|---|
| **Independent Variables** | **No Controls or Fixed Effects (1)** | **No Controls (2)** | **Full Model (3)** |
| Test Variables | | | |
| *BOARD_SIZE* $_{t-1}$ | -0.246*** | -0.189*** | -0.097*** |
| | (-8.382) | (-5.879) | (-2.683) |
| *COMPETENCY* $_{t-1}$ | 2.628* | 2.122 | 3.499* |
| | (1.726) | (1.305) | (1.959) |
| *NETWORK_SIZE* $_{t-1}$ | 0.030 | -0.149 | -0.202* |
| | (0.341) | (-1.548) | (-1.802) |
| *EQUITY_HOLDING* $_{t-1}$ | 0.048*** | 0.060*** | 0.105*** |
| | (3.621) | (4.224) | (6.092) |
| *GENDER_DIVERSITY* $_{t-1}$ | 0.117 | -0.190 | -0.596 |
| | (0.212) | (-0.310) | (-0.894) |
| Control Variables | | | |
| *SIZE* $_{t-1}$ | | | -0.355*** |
| | | | (-6.277) |
| *ROA* $_{t-1}$ | | | 0.023*** |
| | | | (2.817) |
| *LOSS* $_{t-1}$ | | | 0.805*** |
| | | | (3.372) |
| *LEVERAGE* $_{t-1}$ | | | 0.920*** |
| | | | (3.065) |
| *SALES_GROWTH* $_{t-1}$ | | | 0.008** |
| | | | (1.995) |
| *Z_SCORE* $_{t-1}$ | | | 0.027 |
| | | | (1.142) |
| *FIRM_AGE* $_{t-1}$ | | | 0.014*** |
| | | | (3.496) |
| *ACQUISITION* $_{t-1}$ | | | -0.347 |
| | | | (-1.528) |
| *FOREIGN* $_{t-1}$ | | | 0.617*** |
| | | | (4.217) |
| *SEGMENTS_B* $_{t-1}$ | | | 0.272** |
| | | | (2.273) |
| *SEGMENTS_G* $_{t-1}$ | | | 0.099 |
| | | | (0.756) |
| *RESTRUCTURE* $_{t-1}$ | | | -0.012 |
| | | | (-0.087) |
| *NYSE* $_{t-1}$ | | | 0.213 |
| | | | (1.539) |
| *CYBER_RISK* $_{t-1}$ | | | -0.119 |
| | | | (-0.717) |
| Year Fixed Effects | No | Yes | Yes |
| Industry Fixed Effects | No | Yes | Yes |

| | | | |
|---|---|---|---|
| Observations | 1751 | 1751 | 1751 |
| Pseudo $R^2$ | 0.051 | 0.166 | 0.237 |
| Area Under ROC | 0.628 | 0.752 | 0.797 |

Table 7 provides regression results for governance determinants of cybersecurity risk oversight assignment to board-level committee (i.e., audit committee or non-audit committee). The dependent variable in the regression is $OVERSIGHT_{i,t}$, coded as one if oversight is assigned to the audit committee, and zero to non-audit board-level committee(s). Column (1) provides regression results without controls and fixed effects, Column (2) presents results with fixed effects, and Column (3) reports results with controls and fixed effects. The regression includes an intercept but is not tabulated for brevity. Appendix B contains details of these variables. The *t*-statistics are in parentheses and ***, **, and * indicate significance at the 0.01, 0.05, and 0.10 levels, respectively.

TABLE 8 **Descriptive Statistics for Data Breach Sample**

Panel A: Descriptive Statistics for Data Breach Sample (n = 1,656)

| Variable | Mean | Std. Dev. | 25% | Median | 75% |
|---|---|---|---|---|---|
| Test Variables | | | | | |
| *TIME_TO_ANNOUCEMENT* $_t$ (days) | 4.92 | 1.70 | 3.58 | 5.11 | 6.21 |
| *TIME_TO_RESOLUTION* $_t$ (days) | 5.05 | 1.77 | 3.76 | 4.80 | 7.20 |
| *BREACH_FREQUENCY* $_t$ (occurrences) | 2.42 | 1.12 | 2.01 | 3.00 | 3.22 |
| Dependent Variables | | | | | |
| *OVERSIGHT_PREBREACH* $_{t-1}$ (binary) | 0.02 | 0.15 | 0.00 | 0.00 | 0.00 |
| *INFORMATION_TYPE* $_t$ (binary) | 0.87 | 0.34 | 1.00 | 1.00 | 1.00 |
| *NUM_RECORDS* $_t$ | 1.98 | 2.29 | 0.00 | 1.61 | 3.61 |
| *ACTOR* $_t$ (binary) | 0.66 | 0.48 | 0.00 | 1.00 | 1.00 |
| Control Variables | | | | | |
| *SIZE* $_{t-1}$ | 13.11 | 3.07 | 14.43 | 14.64 | 14.71 |
| *ROA* $_{t-1}$ | 1.41 | 1.87 | 0.74 | 1.13 | 1.20 |
| *LOSS* $_{t-1}$ (binary) | 0.01 | 0.09 | 0.00 | 0.00 | 0.00 |
| *LEVERAGE* $_{t-1}$ | 0.10 | 0.06 | 0.08 | 0.09 | 0.10 |
| *CYBER_RISK* $_{t-1}$ (binary) | 0.99 | 0.10 | 1.00 | 1.00 | 1.00 |

Panel B: Other Descriptive Statistics for Data Breach Sample (n = 1,656)

| Variable | Frequency | Percent |
|---|---|---|
| *BREACH_TYPE* $_t$ | | |
| *(1) DATA* | 211 | 12.74 |
| *(2) PRIVACY* | 1011 | 61.05 |
| *(3) OTHER* | 212 | 12.80 |
| *(4) MISSING* | 222 | 13.41 |
| *SOURCE_OF_ATTACK* $_t$ | | |
| *(1) CLIENT_HARDWARE* | 212 | 12.80 |
| *(2) SERVER_CLOUD_WEB* | 1108 | 66.91 |
| *(3) TELECOMMUNICATION* | 125 | 7.55 |
| *(4) PRIVACY_LAW_VIOLATIONS* | 186 | 11.23 |
| *(5) OTHER* | 25 | 1.51 |

Table 8 provides summary statistics for data breach events variables: $TIME\_TO\_ANNOUCEMENT_t$ is the natural log of time to the breach announcement, $TIME\_TO\_RESOLUTION_t$ is the natural log of time to the breach resolution, $BREACH\_FREQUENCY_t$ is the natural log of number of breach events per firm-year, $OVERSIGHT\_PREBREACH_{t-1}$ is an indicator variable for cybersecurity risk oversight assignment prior to a breach event, Type of data, $INFORMATION\_TYPE_t$ is indicator variable for type of information, or assets compromised, $NUM\_RECORDS_t$ is the natural log of records compromised by the breach event, $ACTORS_t$ is an indicator variable for whether cyber-attacks is initiated by internal or external perpetrators, $SIZE_{t-1}$ is the natural log of firms' total assets, $ROA_{t-1}$ is net income scaled by total assets, $LOSS_{t-1}$ is an indicator variable that takes the value of one if net income before extraordinary items is negative, zero otherwise, $LEVERAGE_{t-1}$ is log-term debts scaled by total assets, and $CYBER\_RISK_t$ is an indicator variable for firm's that belong to high cyber risk industries. Panel (B) provides other descriptive statistics for the class variables: $BREACH\_TYPE_t$, which is classified into Data, Privacy, and Other based on Advisen; and $SOURCE\_OF\_ATTACK_t$, which is defined as the source of data, assets, or information that has been compromised, or resulted in the cyber incident and classified as Client Hardware; Server, Cloud, and Web; Telecommunication; Privacy Law Violations; and Others. Appendix B presents definitions of each variable.

TABLE 9 **Pearson Correlation for Data Breach Events Sample**

| | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **1** | *TIME_TO_ANNOUCEMENT* $_t$ | | | | | | | | | | | |
| **2** | *TIME_TO_RESOLUTION* $_t$ | **0.55** | | | | | | | | | | |
| **3** | *BREACH_FREQUENCY* $_t$ | **0.07** | -0.01 | | | | | | | | | |
| **4** | *OVERSIGHT_PREBREACH* $_{t-1}$ | **0.21** | 0.01 | **-0.14** | | | | | | | | |
| **5** | *INFORMATION_TYPE* $_t$ | **0.32** | **0.12** | **0.83** | 0.01 | | | | | | | |
| **6** | *NUM_RECORDS* $_t$ | **-0.16** | **-0.05** | **0.26** | **0.09** | **0.34** | | | | | | |
| **7** | *ACTOR* $_t$ | -0.03 | **0.13** | **0.70** | **0.06** | **0.53** | **0.22** | | | | | |
| **8** | *SIZE* $_{t-1}$ | **0.25** | **0.07** | **0.91** | **-0.16** | **0.87** | **0.16** | **0.62** | | | | |
| **9** | *ROA* $_{t-1}$ | **-0.09** | -0.02 | **-0.26** | **0.38** | **-0.10** | **0.20** | **-0.16** | **-0.36** | | | |
| **10** | *LOSS* $_{t-1}$ | **-0.05** | **0.19** | **-0.14** | 0.03 | **-0.06** | **-0.08** | **-0.11** | **-0.04** | **-0.08** | | |
| **11** | *LEVERAGE* $_{t-1}$ | **-0.05** | -0.01 | **-0.34** | **0.29** | **-0.28** | -0.02 | **-0.22** | **-0.44** | **0.58** | **0.05** | |
| **12** | *CYBER_RISK* $_{t-1}$ | **0.06** | 0.03 | **0.22** | **-0.07** | **0.23** | **0.08** | **0.12** | **0.19** | **-0.39** | **-0.06** | **-0.37** |

Table 9 reports Pearson correlation coefficients for data breach events sample (n = 1,656). Appendix B contains the definitions of the variables. Values in bold indicate statistical significance at 1 percent or better.

TABLE 10 **Impact of Cybersecurity Risk Oversight Responsibility Assignment on Data Breach Consequences**

| | **Dependent Variable** | | | | | |
|---|---|---|---|---|---|---|
| | *TIME_TO_ANNOUCEMENT* $_t$ (days) | | *TIME_TO_RESOLUTION* $_t$ (days) | | *BREACH_FREQUENCY* $_t$ (occurrences) | |
| | (1) | (2) | (3) | (4) | (6) | (7) |
| Test Variable | | | | | | |
| *OVERSIGHT_PREBREACH*$_{t-1}$ | 0.035 | -0.886*** | -2.221*** | -2.038*** | -0.776*** | -0.154*** |
| | (0.811) | (-6.071) | (-17.142) | (-15.121) | (-14.428) | (-2.755) |
| Control Variables | | | | | | |
| *BREACH_TYPE_(DATA)*$_t$ | -5.871*** | -6.223*** | -0.309 | 1.314** | 0.410 | 0.482* |
| | (-0.170) | (-9.063) | (-0.405) | (2.072) | (1.296) | (1.828) |
| *BREACH_TYPE_(PRIVACY)*$_t$ | -4.268*** | -4.407*** | -1.059*** | -1.282*** | -0.867*** | -0.687*** |
| | (-0.008) | (-27.938) | (-7.553) | (-8.802) | (-14.890) | (-11.345) |
| *BREACH_TYPE_(OTHER)*$_t$ | 1.465 | 0.772 | 1.381* | -0.206 | -2.581*** | -2.683*** |
| | (0.626) | (1.172) | (1.897) | (-0.339) | (-8.539) | (-10.623) |
| *SOURCE_OF_ATTACK_(CLIENT_HARDWARE)* $_t$ | 4.320*** | 2.336** | 2.164** | -0.482 | -3.052*** | -1.942*** |
| | (0.409) | (2.434) | (2.139) | (-0.544) | (-7.262) | (-5.273) |
| *SOURCE_OF_ATTACK_(SERVER_CLOUD_WEB)* $_t$ | 1.526 | 0.489 | 2.132*** | 0.345 | -0.586* | -0.790*** |
| | (0.598) | (0.732) | (2.931) | (0.560) | (-1.938) | (-3.084) |
| *SOURCE_OF_ATTACK_(TELECOM)*$_t$ | 3.016*** | 1.061 | 3.542*** | 1.338** | -1.127*** | -0.950*** |
| | (0.316) | (1.524) | (4.766) | (2.082) | (-3.651) | (-3.557) |
| *SOURCE_OF_ATTACK_ (PRIVACY_LAW_VIOLATIONS)* $_t$ | 0.270 | 0.528*** | 2.965*** | 1.992*** | 0.431*** | 0.223*** |
| | (0.145) | (2.723) | (19.712) | (11.118) | (6.901) | (2.998) |
| *INFORMATION_TYPE* $_t$ | -0.536 | -0.923*** | 0.297 | -0.552** | -0.624*** | -0.788*** |
| | (-0.262) | (-3.417) | (1.042) | (-2.213) | (-5.276) | (-7.600) |
| *NUM_RECORDS* $_t$ | 0.058*** | 0.17*** | 0.085*** | 0.121*** | -0.011*** | -0.019*** |
| | (0.003) | (14.161) | (8.959) | (10.945) | (-2.767) | (-4.097) |
| *ACTOR* $_t$ | 1.23*** | 1.272*** | 0.850*** | 0.595*** | 1.366*** | 1.097*** |
| | (0.025) | (9.958) | (6.399) | (5.047) | (24.757) | (22.384) |
| *SIZE* $_{t-1}$ | | -0.201*** | | 0.057** | | 0.156*** |
| | | (-8.046) | | (2.468) | | (16.237) |
| *ROA* $_{t-1}$ | | -0.166*** | | 0.153*** | | 0.001 |
| | | (-10.855) | | (10.806) | | (0.100) |
| *LOSS* $_{t-1}$ | | -2.588*** | | 2.752*** | | -0.505*** |
| | | (-13.567) | | (15.620) | | (-6.905) |
| *LEVERAGE* $_{t-1}$ | | -4.624*** | | -2.218*** | | 2.288*** |
| | | (-11.141) | | (-5.788) | | (14.372) |
| *CYBER_RISK* $_{t-1}$ | | -1.552*** | | 0.937*** | | 0.789*** |
| | | (-7.364) | | (4.811) | | (9.753) |
| Year Fixed Effects | No | Yes | No | Yes | No | Yes |
| Industry Fixed Effects | No | Yes | No | Yes | No | Yes |

| | | | | | | |
|---|---|---|---|---|---|---|
| Observations | 1656 | 1656 | 1656 | 1656 | 1656 | 1656 |
| Adjusted $R^2$ | 0.772 | 0.901 | 0.636 | 0.766 | 0.933 | 0.957 |

Table 10 presents impact of cybersecurity risk oversight assignment on data breach consequences. The dependent variable in Column (1) and (2) is $TIME\_TO\_ANNOUCEMENT_t$, defined as the natural log of the time firm $i$ takes to announce breach in year $t$; dependent variable in Column (3) and (4) is $TIME\_TO\_RESOLUTION_t$, defined as the natural log of the time firm $i$ takes to resolve the breach in year $t$; and dependent variable in Column (5) and (6) is $BREACH\_FREQUENCY_t$ defined as the natural log of number of breach events for firm $i$ in year $t$. The regression includes an intercept but is not tabulated for brevity. Appendix B contains details of these variables. The $t$-statistics are in parentheses and ***, **, and * indicate significance at the 0.01, 0.05, and 0.10 levels, respectively.

**TABLE 11**
**Additional Analysis: Cybersecurity Role, Risk/Compliance/Technology Committee(s), Cybersecurity Framework, Governance Quality, and the Audit Committee as Default Assignment**

| | Dependent Variable: ***OVERSIGHT*** $_t$ | | | | |
|---|---|---|---|---|---|
| | **Level 1** | | | | **Level 3** |
| | Presence of Cybersecurity Role | Presence of RC, CC, and/or TC | Presence of Cybersecurity Framework | Governance Quality | Audit Committee Default Oversight Assignment |
| | (1) | (2) | (3) | (4) | (5) |
| *BOARD_SIZE* $_{t-1}$ | -0.028 | -0.021 | -0.021 | -0.021 | -0.056 |
| | (-1.381) | (-1.065) | (-1.055) | (-1.050) | (-1.389) |
| *COMPETENCY* $_{t-1}$ | 2.284** | 2.573*** | 2.714*** | 2.762*** | 5.220** |
| | (2.358) | (2.671) | (2.816) | (2.864) | (2.357) |
| *NETWORK_SIZE* $_{t-1}$ | 0.406*** | 0.415*** | 0.409*** | 0.413*** | -0.245* |
| | (6.796) | (6.920) | (6.867) | (6.926) | (-1.838) |
| *EQUITY_HOLDING* $_{t-1}$ | -0.015* | -0.015* | -0.016* | -0.016* | 0.074*** |
| | (-1.680) | (-1.654) | (-1.748) | (-1.715) | (3.732) |
| *GENDER_DIVERSITY* $_{t-1}$ | -1.048*** | -1.022*** | -1.039*** | -1.026*** | -0.669 |
| | (-3.076) | (-3.004) | (-3.057) | (-3.014) | (-0.882) |
| *CIO_ROLE* $_{t-1}$ | 0.321*** | | | | |
| | (4.361) | | | | |
| *RISK_COMMITTEE* $_{t-1}$ | | -0.313*** | | | |
| | | (-3.557) | | | |
| *COMPLIANCE_COMMITTEE* $_{t-1}$ | | -0.227** | | | |
| | | (-2.061) | | | |
| *TECHNOLOGY_COMMITTEE* $_{t-1}$ | | -0.148* | | | |
| | | (-1.751) | | | |
| *CYBERSECURITY_FRAMEWORK* $_{t-1}$ | | | 0.511* | | |
| | | | (1.863) | | |
| *INSTITUTIONAL_OWNERSHIP* $_{t-1}$ | | | | 0.156* | |
| | | | | (1.797) | |
| *PRESENCE_OF_RCT* $_{t-1}$ | | | | | -17.432 |
| | | | | | (-0.072) |
| Control Variables | Yes | Yes | Yes | Yes | Yes |
| Year Fixed Effects | Yes | Yes | Yes | Yes | Yes |
| Industry Fixed Effects | Yes | Yes | Yes | Yes | Yes |
| Observations | 7297 | 7297 | 7297 | 7297 | 1751 |

| | | | | | |
|---|---|---|---|---|---|
| Pseudo $R^2$ | 0.374 | 0.374 | 0.373 | 0.373 | 0.386 |
| Area Under ROC | 0.893 | 0.893 | 0.893 | 0.893 | 0.860 |

Table 11 reports regression results of additional tests. The dependent variable ($OVERSIGHT_t$): for Column (1) to (4) is an indicator variable equal to one for firm *i* with an explicit cybersecurity risk oversight assignment in year *t* and zero otherwise*;* and for Column (5) it is an indicator variable equal to one for firm *i* that assigns cybersecurity risk oversight in year *t* to the audit committee and zero if assigned to a non-audit board-level committee(s). Column (1) tests the presence of cybersecurity role ($CYBERSECURITY\_ROLE_{t-1}$) and firms' assignment of cybersecurity risk oversight responsibility, Column (2) tests the presence of $RISK\_COMMITTEE_{t-1}$ (RC), $COMPLIANCE\_COMMITTEE_{t-1}$ (CC), and/or $TECHNOLOGY\_COMMITTEE_{t-1}$ (TC) and firms' assignment of cybersecurity risk oversight responsibility, Column (3) tests the presence of cybersecurity framework ($CYBERSECURITY\_FRAMEWORK_{t-1}$) and firms' assignment of cybersecurity risk oversight responsibility, Column (4) tests the impact of governance quality ($INSTITUTIONAL\_OWNERSHIP_{t-1}$) on firms' assignment of cybersecurity risk oversight responsibility, and Column (5) tests the audit committee's default cybersecurity risk oversight assignment ($PRESENCE\_OF\_RCT_{t-1}$)(level 3 analysis). The regression includes an intercept (similarly for control variables) but is not tabulated for brevity. Appendix B presents details of these variables. The t-statistics are in parentheses and ***, **, and * indicate significance at the 0.01, 0.05, and 0.10 levels, respectively.

## Appendix A

**Section A:** Sample of search result for the term "cyber" in proxy statements (DEF 14A), disclosing the assignment of responsibility for cybersecurity risk oversight.

**Twitter, Inc.** (2020-DEF 14A)
Audit Committee
Risks and exposures associated with financial matters, particularly financial reporting, disclosure controls and procedures, legal and regulatory compliance, financial risk exposures, cybersecurity, cyber risk …. Receives regular reports from management on key cybersecurity, cyber risks, and related issues, including secure processing, storage, and transmission of personal and confidential information, such as the personally identifiable information of people on Twitter.
I assign to the audit committee category.

**Johnson & Johnson** (2020-DEF 14A)
Board Committee Responsibilities
Regulatory Compliance Committee
Compliance with applicable laws, regulations and Company policies related to medical safety, product quality, environmental regulations, employee health and safety, privacy, cybersecurity, and political expenditures. Oversees our risk management programs related to global cybersecurity, information security, product quality, and technology.
I assign to the compliance committee category.

**3M Corp.** (2019-DEF 14A)
Risk Oversight
The Board has delegated to the *Audit Committee* through its charter the primary responsibility for the oversight of risks facing the Company including cybersecurity.
I assign to the audit committee category.

**Fortinet, Inc.** (2018-DEF 14A)
Board's Role in Risk Oversight
The *Board* also directly oversees certain strategic risks to Fortinet and other risk areas not delegated to one of its committees, including risks related to data privacy and cybersecurity.
I assign to the full board category.

**Maxim Integrated Products, Inc. (**2015-DEF 14A**)**
The Board's Role in Risk Oversight
Oversight for regulatory and compliance risks and cyber security are generally shared among board committees … In addition, the chairs of the *Audit Committee and Nominating and Governance Committee* oversee cyber security risks and the Company's initiatives for prevention.
I assign to the joint committee category.

**Inovalon Holdings, Inc.** (2015-DEF 14A)
Risk Oversight
Our *Security and Compliance Committee* monitors the effectiveness of our physical and cybersecurity and related policies, as well as our compliance with legal and regulatory requirements.
I assign to the cybersecurity committee category.

---

**FireEye, Inc.** (2016-DEF 14A)
Risk Management
Finally, our *full board* of directors reviews strategic and operational risk, including but not limited to cybersecurity risk, in the context of reports from the management team, receives reports on all significant committee activities at each regular meeting, and evaluates the risks inherent in significant transactions.
I assign to the full board category.

---

**Section B:** Sample of disclosure of how firms' carry out cybersecurity risk oversight responsibility

---

**Johnson & Johnson** (2020-DEF 14A) page 33
Cybersecurity Oversight
The Regulatory Compliance Committee reviews and receives periodic briefings concerning global cybersecurity, information security, and technology risks, including discussions of any significant cyber incidents, our risk mitigation program and our Company's internal escalation process. The Chief Information Security Officer leads our cybersecurity risk mitigation program, which is fully integrated into the overall enterprise risk management framework and overseen by the Regulatory Compliance Committee".

**Edison International** (2020-DEF 14A) page 15
Cybersecurity Oversight
The Company has identified cybersecurity as a key enterprise risk. Cybersecurity risks are included in the key risk reports to the Audit and Finance Committee discussed above. In addition, the Board has assigned primary responsibility for cybersecurity oversight to the Safety and Operations Committee, which receives regular cybersecurity updates from SCE's Chief Information Officer that focus on cybersecurity threats, defenses, and data analytics that impact the Company's most critical assets. The Board also receives an annual report on cybersecurity from SCE's Chief Information Officer and an independent cybersecurity consultant that includes an assessment of the Company's program and organization.
The Company has established a cybersecurity oversight group comprised of a multidisciplinary senior management team to provide governance and strategic direction for the identification, protection and detection of cybersecurity risks to the Company. Director Trent serves as the Board liaison to the oversight group and regularly attends meetings. Other Board members are invited to attend meetings and typically attend at least one meeting annually.

## Appendix B

### Variable Definitions

| Variable | | Definition [Data Source] |
|---|---|---|
| *ACQUISITION* | = | One if there is an acquisition by firm *i* in year *t* that contributes to sales or net income [Compustat] |
| *ACTORS* | = | Indicator variable for whether internal or external actors initiate cyber-attacks [Advisen] |
| *BOARD_SIZE* | = | Number of board members [BoardEx] |
| *BREACH_FREQUENCY* | = | Natural log of number of breach events for firm *i* in year *t* [Advisen] |
| *BREACH_TYPE* | = | Based on Advisen classification of cyberattacks coded as Data, Privacy, and Other as follows: (1) Data: malicious breach; physically lost or stolen; and unintentional disclosure. (2) Privacy: unauthorized contact or disclosure and unauthorized data collection. (3) Other: industrial controls & operations; IT-configuration/ implementation errors and processing errors; network/website disruption; skimming, physical tampering; identity - fraudulent use/account access; and phishing, spoofing, social engineering. [Advisen] |
| *COMPETENCY* | = | Board cybersecurity competency is measured as a percentage of directors' cybersecurity/IT competency and experience. A director is deemed to have IT experience if they have professional work experience as a CIO, CSO, CISO, or director, vice president, senior vice president, head, manager, or general manager of information technology, information, information services, information systems, or information management [BoardEx] |
| *COMPLIANCE_COMMITTEE* | = | An indicator variable equals to one if firm *i* discloses the presence of a "compliance committee" at the board-level in year *t* prior to the date of the breach, or zero otherwise [BoardEx] |
| *CYBERSECURITY_FRAMEWORK* | = | One if firm *i* adopts one of the cybersecurity frameworks including NIST, COBIT, ISO/IEC 27001/27002, AICPA Trust Services Criteria, etc. in year *t*, and zero otherwise [Proxy Statements- DEF 14A] |
| *CYBER_RISK* | = | One if firm *i* belongs to one of the following industries: financial services, healthcare, retail, manufacturing, or information and communications in year *t*, and zero otherwise (NAICS 31, 32, 33, 44, 45, 51, 52, and 62) |
| *CYBERSECURITY_ROLE* | = | One if firm *i*'s top management team has a CIO, Chief Security Officer (CSO), Chief Security Information Officer (CSIO), Chief Privacy Officer (CPO), Chief Risk Officer (CRO), VP of Information, Director of IT, or IT Director in year *t* (zero otherwise) [Proxy Statements- DEF 14A] |
| *FIRM_AGE* | = | The age of firm *i* in years as of year *t* [Compustat] |
| *FOREIGN* | = | One if firm *i* has non-zero pre-tax foreign income in year *t*, and zero otherwise [Compustat] |
| *GENDER_DIVERSITY* | = | Board gender diversity measured as percentage of firm *i* female directors in year *t* [BoardEx] |
| *INFORMATION_TYPE* | = | Type of data, information, or assets compromised coded as *Corporate* including Corporate Loss of Business Income/Services, Corporate Loss of Digital Assets, and |

| Variable | | Definition [Data Source] |
|---|---|---|
| | | Corporate Loss of Financial Assets, and *Personal* covering: Personal Financial Identity, Personal Health Information, and Personal Identity Information [Advisen] |
| *INSTITUTIONAL_OWNERSHIP* | | Number of shares held by institutional shareholders that own more than 5% of a firm's equity to total number of shares outstanding [Thomson-Reuters 13F] |
| *LEVERAGE* | = | long term debt scaled by total assets for firm *i* in year *t* [Compustat] |
| *LOSS* | = | One if firm *i* exhibits net income less than zero in year *t* and zero otherwise [Compustat] |
| *NETWORK_SIZE* | = | Board network size calculated as log of the aggregate of connections for each director from the BoardEx database at the board level. This measure of board networks simply counts the number of first-degree links for all directors on the board including board connections through educational institutions attended, current and previous employers, military service as well as civic institutions like non-profit boards [BoardEx] |
| *NUM_RECORDS* | = | Natural log of number of identities breached or stolen, social security numbers revealed, devices compromised, etc. [Advisen] |
| *NYSE* | = | One if a firm *i* is listed on the New York Stock Exchange in that year *t*, and zero otherwise |
| *OVERSIGHT* | = | Board or board-level committee(s) responsible for overseeing the cybersecurity in firm *i* in year *t*. There are ten categories of oversight responsibility: full board, audit committee, finance committee, technology committee, compliance committee, risk committee, joint committee, cybersecurity committee, nominating and governance committee, and other [Proxy Statements- DEF 14A].<br>The cybersecurity risk oversight responsibility assignment **level 1,** *OVERSIGHT* is an indicator variable equal to one for firm *i* with an explicit cybersecurity risk oversight assignment in year *t* and zero otherwise.<br>The cybersecurity risk oversight responsibility assignment **level 2**, *OVERSIGHT* is an indicator variable equal to one for firm *i* that assigns cybersecurity risk oversight in year *t* to the full board and zero if assigned to a board-level committee(s).<br>The cybersecurity risk oversight responsibility assignment **Level 3**, *OVERSIGHT* is an indicator variable equal to one for firm *i* that assigns cybersecurity risk oversight in year *t* to the audit committee and zero if assigned to a non-audit board-level committee(s). |
| *OVERSIGHT_PREBREACH* | = | Same as OVERSIGHT except it is defined for firms that have an explicit cybersecurity risk oversight assignment ***before*** the cybersecurity breach incident |
| *PRESENCE_OF_RCT* | = | An indicator variable equal to one if firm *i* discloses the presence of any one of risk, compliance, and/or technology committees at the board-level in year prior to the date *t* of the breach, or zero otherwise [BoardEx] |
| *RESTRUCTURE* | = | One if firm *i* restructures any part of its business in year *t*, and zero otherwise [Compustat] |
| *ROA* | = | Net income scaled by total assets for firm *i* in year *t* [Compustat] |

| Variable | | Definition [Data Source] |
|---|---|---|
| *RISK_COMMITTEE* | = | An indicator variable equal to one if firm *i* discloses the presence of a "risk committee" at the board-level in year prior to the date *t* of the breach, or zero otherwise [BoardEx] |
| *SALES_GROWTH* | = | Sales for firm *i* in year t minus sales for firm *i* in year *t-1*, all scaled by sales for firm *i* in year *t-1* [Compustat] |
| *SEGMENTS_B* | = | Number of business segments for firm i in year *t* [Compustat] |
| *SEGMENTS_G* | = | Number of geographic segments for firm i in year *t* [Compustat] |
| *SOURCE_OF_ATTACK* | = | Source of data, assets, or information that has been compromised, or resulted in the cyber incident. Coded as: (1) Client Hardware; (2) Server, Cloud, and Web; (3) Telecommunication; (4) Privacy Law Violations; and (5) Others. [Advisen] |
| *SIZE* | = | Natural log of firm *i*'s total assets in year *t* [Compustat] |
| *TECHNOLOGY_COMMITTEE* | = | An indicator variable equal to one if firm *i* discloses the presence of a "technology committee" at the board-level in year *t* prior to the date of the breach, or zero otherwise [BoardEx] |
| *TIME_TO_ANNOUCEMENT* | = | Natural log of number of days between incident date and first notice date of a breach for firm $i$ in year $t$ [Advisen] |
| *TIME_TO_RESOLUTION* | = | Natural log of number of number of days between original loss start date and original loss end date of a breach for firm $i$ in year $t$ [Advisen] |
| *Z_SCORE* | = | Modified Altman (1968) Z-score = (1.2*working capital + 1.4*retained earnings + 3.3*income before extraordinary items + 0.999*sales)/total assets [Compustat] |

## Chapter 4: Disclosure of Cybersecurity Risks Transfer and Data Breaches


### Abstract

The increase and severity of data breaches lead firms to adopt various risk management strategies including transferring such risk via cyber insurance to reduce potential costs of a data breach. This study examines the relation between cyber insurance disclosure and a firm's likelihood of being the target of a future breach. Using textual analysis of the risk factors of 10-K filings during the period 2010–2021 and comparing cyber insurance disclosures of firms that were breached to others that were not, the study finds that firms mentioning the existence of cyber insurance have a significantly higher subsequent probability of being breached relative to firms that do not do so. This finding indicates that cyber insurance disclosure attracts unwanted attention from hackers. To obtain further evidence on the effectiveness of cyber insurance in the event of an actual breach, the study finds that cyber insurance leads to delayed public breach disclosure, more timely breach resolution, and higher breach recurrences. The study adds to the literature on disclosure and cybersecurity, while also informing practitioners as they evaluate the effectiveness of cybersecurity risks counter mechanisms, particularly since disclosure of cyber insurance is voluntary.



**Keywords:** Cybersecurity, cyber insurance, disclosure, data breaches, risk management, risk transfer


### 4.1 Introduction

Cybersecurity risks are increasing at an alarming rate as organizations amass huge amounts of electronic data (Lieberman 2017). Beyond the loss of data, a cyber breach has potentially serious implications on a firm's intellectual property, reputation, market value, customer trust and confidence, brand switching, audit fees, etc. (Campbell et al. 2003; He et al. 2020; Huang and

Wang 2021; Kamiya et al. 2021; Li et al. 2020; Martin et al. 2017; Smith et al. 2019). Additionally, it can cause extensive consequences that extend beyond the company itself, such as influencing the supply chain (Crosignani et al. 2023), financial infrastructure (Kopp et al. 2017), and overall economy (Eisenbach et al. 2022). To hedge against cybersecurity risks, an emerging option is the purchase of cyber insurance, which transfers such risks to an insurer.[16] The objective of this study is to examine the relation between firms disclosing their cyber insurance and the likelihood of a data breach as well as the relation between firms disclosing their cyber insurance and breach consequences.

The study focuses on cyber insurance for several reasons. First, the U.S. cyber insurance market is currently worth more than $3 billion annually and is estimated to grow between two- to seven-fold over the next decade (PwC 2021; Coker 2021). While less than half of organizations had cyber insurance in 2016, that number increased to nearly two-thirds in 2019 specifically protecting against cyber and data theft losses (Maurer et al. 2021).[17] Second, unlike the traditional risk management mechanisms of mitigating, accepting, and avoiding risk, cyber insurance is believed to provide a stronger overall cybersecurity solution (Shackelford 2012), offering not only risk transfer but also risk response in the event of a cyber breach.[18] Third, cyber insurance can be an important component of a firm's cybersecurity risk management policies and procedures, which are key elements of enterprise-wide risk management and essential for ensuring compliance with federal securities laws (SEC 2018) and maintaining the reliability of financial reporting (Cohen et

[16] Cyber insurance is defined as "insurance contracts designed to mitigate liability issues, property loss and theft, data damage, loss of income from network outage and computer failures, Web-site defacement, and cyberextortion" (Bandyopadhyay et al. 2009).
[17] 414 unique organizations, regardless of listing status, responded to the survey.
[18] The difference between cyber risk transfer and mitigation is that the former relates to cybersecurity risks that fall outside the tolerance levels and that can be reduced to "an acceptable level by sharing a portion of the consequences with another party", while the latter relates to "actions and security controls that reduce the threats, vulnerabilities, and impacts of a given risk to an acceptable level" (Stine et al. 2020).

al. 2017). Fourth, there is a growing need to proactively manage cybersecurity risks (NIST 2018; Sonnemaker 2019), especially since firms are currently generally underprepared (Maurer et al. 2021; PwC 2018) and are mainly reactive to such risks. In this respect, cyber insurance is used as a tool for proactively addressing cybersecurity risks. Fifth, cyber insurance may serve as an indicator of protection and as a motivator for organizations to increase their preventive investments (Panda et al. 2021). Finally, a better understanding of cyber insurance contributes to better control of insurance premiums (SEC 2018), and the development of new and improved cybersecurity regulation (Panda et al. 2021), such as the proposed California State Assembly-Bill 2320, which would require businesses that keep customer information to maintain cyber insurance coverage (Hobson and Adams 2020).

Firms opt for cyber insurance to improve their cybersecurity "due care" (Bonner 2012), mitigate the influence of data breach costs (IBM 2020; Mittel 2020), and access insurance providers' services of responding, investigating, and defending against the consequences of a data breach (Talesh 2018). In other words, firms purchase cyber insurance for economic, risk strategy, and/or access to knowledge reasons (Boyer 2014; Frank et al. 2021). However, the underestimation of cyber insurance importance (Kshetri 2020), and fear of false sense of control and coverage (Eling and Schnell 2016; Kabir et al. 2020) downplay the effectiveness of cyber insurance policy. The high premiums, confusion on the scope of coverage, and difficulty of estimating the probability of attacks and potential losses (Bodin et al. 2018; Francis et al. 2021; Koijen and Yogo 2022) present further challenges for clients in the nascent cyber insurance market.

On the one hand, it can be expected that firms disclosing cyber insurance coverage, as encouraged by the Securities and Exchange Commission (SEC) (SEC 2011), signal their commitment to cybersecurity issues, risk management, and a better understanding of their risks

(Gordon et al. 2010). Moreover, such disclosure potentially minimizes cybersecurity risks as well as overall cybersecurity information asymmetry with capital markets (Gao et al. 2020; Jiang et al. 2021). On the other hand, disclosure of cyber insurance may attract unwanted attention from hackers, thus further exposing a firm to cyberattacks (Havakhor et al. 2020) which may, in turn, diminish a firm's incentive to disclose its cyber risk management initiatives. Hence, under this scenario, firms may view disclosure of cyber insurance as bearing higher costs compared to its benefits (Verrecchia 1983; 2001) and thus opt not to disclose on their cyber insurance. Therefore, the relationship between the joint probability of having cyber insurance and disclosing it and the likelihood of breaches is not clear and is an empirical question. However, it is challenging to accurately estimate this joint probability, as it is not possible to know for sure that all firms having insurance will disclose it. This situation is even more complicated by the fact that hackers share information through the dark web which may be a factor, separately from cyber insurance, that impacts the breach status of a given firm. Cybercrime is indeed becoming more of a sophisticated form of business. Even under such circumstances, some firms disclose their cyber insurance in compliance with the SEC 2011 and 2018 guidance on cybersecurity risks and incidents disclosure; specially when firms are breached.[19]

Focusing on "Item 1A. Risk Factors" section of 10-K filings during the period 2010-2021, a two-stage textual analysis is used to identify and search for key terms that proxy for cyber insurance disclosure. Reliance on 10-K filings rests on SEC cybersecurity guidance, which recommends that cybersecurity risks disclosure includes a "description of relevant insurance

[19] To mitigate this issue, the study examines breached firms that disclosed their cyber insurance post a breach event, in compliance with the SEC requirement that firms disclose insurance information as part of a cyber incident disclosure. Excluding such firms, the results support the main findings of positive association between the disclosure of cyber insurance and probability of a breach.

coverage" (SEC 2011).[20] Combining the results of the cyber insurance disclosure search with the cyber breach status obtained from Advisen Ltd.'s proprietary dataset, the analysis reveals that disclosing cyber insurance increases the likelihood of a breach event by 51 percent.[21] This finding may indicate that disclosure of cyber insurance attracts unwanted attention from hackers, or that firms with such insurance are paying less attention to safeguard against cyber breaches, or both. Although cyber insurance disclosure and number of breaches are more pronounced in the finance sector, the main inference persists across financial and non-financial sector analysis. Furthermore, the main inference holds controlling for the length of risk disclosure section, high-intensity IT setting, assets tangibility structure, and internal control weaknesses.

Further analysis examines the effectiveness of cyber insurance in the event of an actual cyber breach, namely the association between disclosure of cyber insurance and the timeliness of breach announcement, resolution, and its frequency. Cyber insurance may shorten the time firms take to announce and/or resolve the breach by providing access to insurers' services beyond financial protection of incident response, communication, and legal expertise (Talesh 2018).[22] However, cyber insurance may prolong the time to the breach announcement and/or resolution as insurance providers take time to investigate and determine whether the event is covered by the policy and to establish the extent of the resulting liability.

[20] Although, SEC Regulation S-K Item 305 does not mention cybersecurity risks, it mandates that firms must disclose in the "Item 1A. Risk Factors" section accurate description of the most significant risks they are exposed to and how such risks affect their operations.

[21] The Advisen Cyber Loss Data is a proprietary database that covers cybersecurity incidents around the world. The data is collected from varied sources (SEC filings, press releases, business press and newspaper articles, court rulings, etc.). This dataset is more comprehensive than the publicly available and widely used Privacy Rights Clearinghouse. It provides detailed information of cyber events, including case type, case status, event disclosure date, information being compromised, breached date, number of records being affected, actors, source of loss, type of loss, and amount of loss, among others. For more information: https://www.advisenltd.com/about/

[22] A recent report by IBM (2020) highlights that "51% of organizations with cyber insurance used claims to cover the cost of third-party consulting and legal services."

As for breach frequency, cyber insurance may decrease a firm's exposure to cyber breaches as it is usually extended to eligible firms after a series of evaluation assessments of their existing security measures and practices (Bonner 2012), and the insurance bridges firm's cybersecurity competency or knowledge gap by providing risk management services (Talesh 2018). However, it is also possible that cyber insurance may not decrease the frequency of cyber incidents as it may draw the attention of cybercriminals to not only the possibility of weaknesses in the firm's cyber defenses but also the ability of a firm to afford payment for extortion demands (Cimpanu 2020; Havakhor et al. 2020). Furthermore, cyber insurance may reduce firms' incentives to invest in self-protection measures (Eling and Schnell 2016).

The results of the breach sample analysis indicate that cyber insurance impacts the consequences of a breach. More specifically, firms disclosing cyber insurance take longer time to disclose the breach by an average of 1.12 days. This finding supports the notion that firms are not benefiting from the expertise of their insurance providers for timely breach disclosure, or that the time overhead of accessing insurance providers expert counseling and legal expertise represents a delaying factor in the breach announcement, or both. However, the results further indicate that holding cyber insurance reduces on average the time firms take to resolve and contain the breach by 1.4 days. This finding highlights that cyber insurance benefits firms by providing access to the insurance providers' expertise in handling the aftermath of a breach in a more timely manner. Regarding breach recurrence, the results indicate a positive relation between cyber insurance and breach frequency, supporting the main finding that disclosing cyber insurance may expose firms to becoming targets of future breaches. Finally, a cross-industry sector analysis shows that business equipment and software; and healthcare industries demonstrate better capacity to resolve breaches and all industry types are similarly impacted vis-a-vis the recurrence of a breach.

To address the endogeneity and selection bias issues, the study uses alternative approaches including a propensity score matching (PSM), two stage least squares (2SLS) with instrumental variables, and Heckman (1979) two-stage model. Overall, the study's main inferences of the positive association between cyber insurance and probability of a future breach remains unchanged using these alternative endogeneity approaches.

This study makes the following contributions. First, it contributes to filling a gap in empirical research on cyber insurance which is currently scant. Recent studies only tangentially touch on cyber insurance disclosure. Namely, Florackis et al. (2023), in the context of developing a text-based measure of cyber risk disclosure, report that firms with more cyber risks exposure actively manage such risks through the disclosure of their cyber insurance policy. Using earnings calls, Jamilov et al. (2021) document that text-based measures of cyber risk can predict future realized cyberattacks and that inclusion of "insurance and legal" discussion slightly increases the probability. The current study is similar to both studies in that it utilizes textual analysis, examines the same disclosure outlet as Florackis et al. (2023) (Item 1A. Risk Factors), but employs more comprehensive and inclusive search strategies. Furthermore, the study is different in that cyber insurance disclosure is its core topic of analysis and that the study goes beyond establishing the positive association between cyber insurance and the probability of being the target of a breach to examining the effectiveness of cyber insurance disclosure on the consequences of an actual breach.

Second, while prior research on cybersecurity focuses mainly on post-breach impacts (Campbell et al. 2003; Huang and Wang 2021; Li et al. 2020; Martin et al. 2017), this study contributes to both pre- and post-impacts of a cybersecurity risk management strategy, namely risk transfer via cyber insurance. At the pre-breach level, the study examines the relation between cyber insurance disclosure and the likelihood of a breach event, thus the study adds to the growing

literature that studies the determinants of occurrences of cyber breaches (Ettredge et al. 2018; Florackis et al. 2023; Higgs et al. 2016; Jamilov et al. 2021; Kamiya et al. 2021). In particular, the study finds that disclosure of the presence of cyber insurance in a firm's annual report is positively associated with subsequent breaches. At the post-breach level, the study sheds light on the effectiveness of cyber insurance as a risk management strategy on the timeliness of breach announcement and resolution as well as breach recurrence, thus the study adds to the literature that studies the effectiveness of firms' risk management strategies (Biener et al. 2015; Eling and Wirfs 2019; Schoenfeld 2022).

Third, this study contributes to the literature on corporate disclosure policies. While the SEC (2018) emphasizes that "disclosures regarding a company's cybersecurity risk management program […] allow investors to assess how a board of directors is discharging its risk oversight responsibility", this study, similar to Ettredge et al. (2018), provides managers with an additional factor to consider when determining their disclosure policy. Specifically, it suggests that revealing the presence of cyber insurance may serve as an incentive for potential cyberattacks.

Fourth, the study answers recent calls for research on cyber insurance (Koijen and Yogo 2022), particularly, the call to investigate whether cyber insurance leads to fewer cyber incidents (Talesh 2018) and whether cyber insurance is an effective risk management tool (Janvrin and Wang 2022; Walton et al. 2020). Finally, this study offers practical insights on how the disclosure of cyber insurance relates to the likelihood of a breach, time to a breach announcement and resolution as well as the frequency of data breaches. The findings of this study also inform practitioners, regulators, and policy makers as they evaluate their cybersecurity risks strategy and the effectiveness of their cybersecurity risks counter measures, especially since disclosure of cyber insurance is voluntary.

The rest of the paper is organized as follows. Section 2 reviews the relevant literature and develops the hypotheses. Section 3 details sample selection and empirical research design. Section 4 discusses the results of tests, and Section 5 concludes.

## 4.2 Background and hypotheses development

### 4.2.1 Regulatory background on cyber insurance disclosure

In the fight against cybercrime, cybersecurity insurance is put forward as a critical tool in an organization's risk management strategy. For example, the U.S. Department of Commerce indicates that a company's cybersecurity preparedness may include cybersecurity insurance (Aguilar 2014). In addition, the U.S. Department of Homeland Security reports the vital role of cyber insurance especially that "a robust cybersecurity insurance market could help reduce the number of successful cyberattacks by promoting the adoption of preventative measures in return for more coverage; and encouraging the implementation of best practices by basing premiums on an insured's level of self-protection" (DHS 2017).

Firms are also increasingly pressured by legislators to better protect personal information about customers, clients, suppliers, employees, etc. For example, the California Consumer Privacy Act (CCPA), state-level Security Breach Notification Laws (SBNLs) in the U.S., and the European Union (EU) General Data Protection Regulation (GDPR) are requiring firms to update their cybersecurity measures and practices to enable compliance (Biros et al. 2019; Klein et al. 2022; Shackelford 2012). For example, many firms reported purchasing cyber insurance following the enactment of the CCPA (Stoller 2020). Based on these laws, courts are increasingly willing to hold organizations liable for not protecting private information (Shackelford 2012). For example, the SEC fined London-based educational publishing company Pearson PLC $1 million to settle charges for misleading investors about a 2018 intrusion (Greenwald 2021). Similarly, Equifax paid

$575 million to settle with the Federal Trade Commission, the Consumer Financial Protection Bureau, and all 50 U.S. states and territories over its "failure to take reasonable steps to secure its network" (Swinhoe 2022). The coercive institutional pressure and litigation risks over the protection of information assets under a myriad of laws may pressure companies to increase the scope of cyber insurance coverage to reduce cyber incident costs.

Even if firms purchased cyber insurance, disclosure of such coverage is encouraged but not mandated by the SEC.[23] Specifically, the SEC encourages firms to disclose their cyber insurance stating that appropriate disclosures of cybersecurity risks and cyber incidents may include "a description of relevant insurance coverage" (SEC 2011) and "costs associated with maintaining cybersecurity protections, including, if applicable, insurance coverage relating to cybersecurity incidents or payments to service providers" (SEC 2018).[24] The SEC monitors and requests more information about the disclosure of cyber insurance coverage in the event of a cyber incident. For example, the SEC requested Alion Science and Technology Corporation to revise its 2014 cybersecurity incident disclosure and further describe its cyber insurance policy, including material limits on coverage "[s]o that an investor is better able to understand the materiality of the cybersecurity incident." [25]

### 4.2.2 Relevant literature

The literature on cyber risk insurance is mainly analytical, addressing, for example, the use of cyber insurance to minimize cyber risk losses (Gordon et al. 2003), determination of cyber risk premium (Mukhopadhyay et al. 2013), selection among cyber insurance, self-insurance, or self-

[23] The SEC has issued cybersecurity guidance in 2011 and interpretive guidance in 2018 on disclosure obligations relating to cybersecurity risks and cyber incidents (SEC 2011; 2018).
[24] Recently, Blackbaud, Inc. disclosed in its filing information on receivables for probable cyber insurance recoveries following a ransomware attack in May 2020.
[25] For more detail see SEC comment letter (Form S-1) to Alion Science and Technology Corporation https://www.sec.gov/Archives/edgar/data/1166568/000000000014012655/filename1.pdf

protection (Mukhopadhyay et al. 2019), and selection of an optimal set of cyber insurance policies (Bodin et al. 2018) (see Eling and Schnell (2016) for a detailed review of the cyber risk insurance literature).

An examination of a broad literature in different disciplines including finance, information systems, law, insurance, and cybersecurity, uncovers only a few cyber insurance empirical studies and thus reveals a clear gap in empirical research on cyber insurance.[26] Biener et al. (2015) examine the insurability of cyber risk based on actual cyber loss data and actuarial science methods. The study highlights empirically the distinct characteristics of cyber risks, especially the highly interrelated losses, lack of data, and severe information asymmetries, that deter the development of a sustainable cyber insurance market. However, Talesh (2018) highlights the importance of cyber insurance as a mechanism to comply with privacy laws and to deal with data breaches, as insurance companies act as compliance overseers and managers for organizations dealing with cybersecurity threats. Recent research indicates that cyber insurance attenuates the market reaction to cybersecurity breach incidents by absorbing cybersecurity breach costs (Haislip et al. 2019).

Romanosky et al. (2019) highlight weaknesses in the content of cyber insurance policies such as lack of a clear distinction between first- and third-party losses coverage, lack of coverage for risks from emerging technologies (e.g., mobile devices and IoT devices), and lack of consideration for using frameworks for information technology management (e.g., COBIT, NIST, or ISO 27001/2) or the maturity of technical, business, and security infrastructure. Perhaps one way to mitigate the weakness in such cyber insurance policies is to incorporate the recommendations of Palsson et al. (2020) that are based on the descriptive analysis of Advisen

[26] See Boyer (2020) for recent empirical papers focusing mainly on supply and demand of cyber insurance.

Ltd. data set. Despite these weaknesses, companies commit to cyber insurance as a risk management strategy in response to institutional pressures and even to appease investors and regulators (Ogbanufe et al. 2021).

Focusing on cybersecurity disclosure literature, prior research indicates that firms generally update their cyber risks disclosure after they suffer cyberattacks. The nature of such disclosure ranges from focusing on less severe attacks (Amir et al. 2018), obfuscating the incident (Jackson et al. 2019), reflecting the impact of prior breaches and how the market reacts to such breaches (Jiang et al. 2021), and focusing less on incident control, risk mitigation, and business continuity (Cheong et al. 2020). Interorganizational relationships also impact firms' behavior towards cybersecurity risks disclosure in that supply chain cyber risk is an important determinant of the demand for assurance of such risk management processes (Hampton et al. 2021).

Furthermore, cybersecurity risks disclosure focuses more on risk mitigation than risk transfer. Gordon et al. (2010) examine the market value of information security voluntary disclosures and find a positive association between the voluntary disclosure of items concerning information security and the market value of a firm. In addition, Wang et al. (2013) find that firms that disclose actionable cyber risk-mitigating information in their security risk factors disclosure are less likely to be associated with future breach incidents. Berkman et al. (2018) document that weak cybersecurity risks mitigation in annual reports opens opportunities for the acquisition of private information and trading by privately informed traders.

Recent studies that examine cybersecurity risks disclosure address cyber insurance disclosure only tangentially (Héroux and Fortin 2020; Florackis et al. 2023; Jamilov et al. 2021). Héroux and Fortin (2020, p. 83), focusing on content of cybersecurity disclosure, report that the number of Canadian firms disclosing cyber insurance is low but do not seek to further investigate

this phenomenon. Similarly, Florackis et al. (2023), in the context of developing a measure of cybersecurity risks disclosure, find that firms with more cyber risks exposure actively manage such risks through the disclosure of their cyber insurance policy. Furthermore, using earning calls, Jamilov et al. (2021) develop a text-based firm-level measures of cyber risk exposure and classify cyber risk discussions into 11 topics including "legal and insurance". The study documents that text-based measures of cyber risk can predict future realized cyberattacks and that inclusion of "insurance and legal" discussion slightly increases the probabliy. The study contributes to the emerging literature on cybersecurity by explicitly focusing on cyber insurance disclosure from an empirical point of view.

### 4.2.3 Hypotheses development

Cyber insurance offers an economic alternative to the economically infeasible option of firms fully protecting all systems (Anderson et al. 2012; Bandyopadhyay et al. 2009). Furthermore, the purchase of cyber insurance improves a firm's cybersecurity "due care" (Bonner 2012), mitigates the influence of data breach costs (Gordon et al. 2003; IBM 2020; Mittel 2020), and supports firms in responding to regulatory inquiries or fines (Hobson and Adams 2020). A derivative benefit of cyber insurance is that it goes beyond risk transfer and provides access to services for responding to, investigating, defending, and mitigating against the consequences of a data breach (Talesh 2018).

There is, however, skepticism over the effectiveness of cyber insurance. Many firms underestimate the importance of cyber insurance (Kshetri 2020), while others fear the false sense of control resulting from maintaining cyber insurance (Eling and Schnell 2016; Kabir et al. 2020). Reliance on cyber insurance could expose organizations to more risks as a result of their belief that insurers bear the resulting financial liability (Kabir et al. 2020). However, cyber insurance

coverage is limited only to direct breach costs and excludes indirect costs such as reputation damage, customer loss, increase of cost of capital, and insurance premiums (Boasiako and Keefe 2021; Kopp et al. 2017).[27] Moreover, there is a multitude of challenges associated with the nascent cyber insurance market (Bodin et al. 2018) including, high premiums and overpricing, confusion on the scope of coverage (Bandyopadhyay et al. 2009; Kshetri 2020), limited coverage for some industry sectors, such as healthcare (GAO 2021), and lack of sufficient historical data to develop actuarial models for estimating the probability of attacks and potential losses (Francis et al. 2021). Furthermore, there is a misconception that general liability insurance coverage extends to cyber-attack losses (Bodin et al. 2018; Bonner 2012).[28] Therefore, the study expects that such tension influences a firm's decision to purchase cyber insurance.

Firms that purchase cyber insurance may choose to voluntarily provide disclosure on their cyber insurance policy in their regulatory filings. On the one hand, cyber insurance disclosure may serve to reflect a firm's attempt to manage cybersecurity risks, to signal its active commitment to cybersecurity issues (Gordon et al. 2010), to minimize cybersecurity risks and overall cybersecurity information asymmetry with capital markets participants and other stakeholders (Gao et al. 2020; Jensen and Meckling 1976; Jiang et al. 2021), and to reduce litigation costs by increasing transparency, thus lowering liability (Kasznik and Lev 1995; Skinner 1997). Furthermore, disclosure of cyber insurance provides granular information about a firm's cybersecurity risks management, enabling investors to better evaluate the fundamental value of the firm (Gal-Or and Ghose 2005). Hence, the study expects investors' belief with respect to firms

[27] For example, Verizon Communications Inc discloses in its 10-K for fiscal year 2017, that "the potential costs associated with these attacks could exceed the insurance coverage we maintain."
[28] In a famous hacking incident in 2011, Sony corporation, believing that it is covered under its commercial general liability, lost its case against Zurich American Insurance Company on the grounds that its commercial general liability coverage does not extend to losses resulting from data breaches (Bonner 2012).

that provide cyber insurance disclosure to be that they better understand their risks and can adopt more effective countermeasures to reduce cybersecurity risks (Berkman et al. 2018) and the likelihood of data breaches.

On the other hand, disclosure of cyber insurance may attract unwanted attention from hackers, thus further exposing a firm to cyberattacks (Havakhor et al. 2020). In turn, this possibility diminishes the firm's incentive to disclose its cyber risk management initiatives. For example, there is a call for banning cyber insurers from indemnifying ransom payments (Sabbagh 2021) as firms are not only more likely to pay if insurers indemnify some or all the payment but also more likely to impose a negative externality on peers who now face a higher threat level. Such possibility is aggravated by the fact that ransomware attacks make up almost half of all cyber insurance claims (Cimpanu 2020 relying on first half of 2020 numbers). Accordingly, firms may view disclosure of cyber insurance as bearing higher costs compared to the benefits (Verrecchia 1983; 2001) and thus do not disclose on their cyber insurance. Therefore, the relationship between the joint probability of having cyber insurance and disclosing it and the likelihood of cybersecurity breaches is not clear ex ante. Hence, the first hypothesis, stated in null form, is as follows:

> **Hypothesis 1** (H1): *The disclosure of cyber insurance is not associated with the likelihood of a subsequent data breach.*

To understand the effectiveness of cyber insurance in the event of a breach, the study examines the association between cyber insurance disclosure and the time a firm takes to announce or resolve the breach, as well as the recurrence of a breach. The relationship between cyber insurance disclosure and timeliness of breach announcement and resolution is not clear. On the one hand, one can argue that cyber insurance may facilitate timely disclosure and resolution of breach events. Cyber insurance often provides services beyond financial protection, including expert consulting services to handle quick incident response, help to formulate communication about the incident,

and access to legal expertise (Talesh 2018). Consequently, these services can enhance firms' cybersecurity resilience and assist in meeting their compliance with the SEC's mandates for timely material breach disclosure and requirement for transparency and accountability. Furthermore, they may also facilitate timely resolution for breaches. For example, an IBM (2020) report highlights the utility of cyber insurance in that "51% of organizations with cyber insurance used claims to cover the cost of third-party consulting and legal services". Hence, cyber insurance may shorten the time to the breach announcement and/or resolution. However, cyber insurance providers may prolong the process of breach event announcement to delay the payment of the coverage to the policyholders as much as possible.[29] In addition, insurance providers will need to thoroughly investigate the incident to determine whether the event is covered by the policy and if so, establish the extent of resulting liability. Such investigation and associated legal wrangling may contribute to the delay of the breach announcement and resolution. The SEC's guidance on timely disclosure of material cyber breaches serves as a valuable tool to ensure that investors have access to accurate and up-to-date information about a company's material events. However, it is important to note that the SEC's four business day requirement is not a comprehensive prescription for all cyber breaches, and firms are required to assess the materiality of each breach and decide about whether it must be reported. Yet it is still possible that cyber insurance providers may prolong the process of breach event announcement. Particularly, Foerderer and Schuetz (2022) find that firms strategically time breach announcements to coincide with predictably busy days in the media to attenuate investor reactions.

[29] Although the SEC requires disclosure of material events, it encourages companies to use Form 8-K to report material breaches. However, this requirement is subject to firms' materiality assessments, hence some companies may delay disclosure until their next quarterly or annual filing, and as a result, it does not undermine the possibility that cyber insurance providers prolonging the announcement of a breach. In addition, firms may use their discretion (Jorgensen and Kirschenheiter 2003) when deciding whether to publicly report data breaches and may rationalize that a breach does not meet the qualifications for an immediate financial disclosure, hence many major breaches are first disclosed by the media (Freifeld 2014; Shumsky 2016).

Similarly, the relationship between cyber insurance disclosure and breach frequency is not clear. Cyber insurance providers extend coverage based on an organization's eligibility after conducting a series of health checks and scans of its employees, technologies, processes, and networks (Talesh 2018). The assessments aim to confirm the adequacy of a firm's security measures and practices to grant it coverage (Bonner 2012) at a better premium (Panda et al. 2021). Furthermore, cyber insurance provides risk management services that fill an organization's cybersecurity competency or knowledge gap (Talesh 2018), which may translate into reducing the frequency of cyberattacks. Thus, ensuring the adequacy of security measures and practices, for the purpose of taking out cyber insurance, may strengthen defenses against cyberattacks and reduce the frequency of cyber breaches. However, disclosure of cyber insurance may expose firms to cyberattacks by drawing the attention of cybercriminals to the possibility of weaknesses in the firm's cyber defenses and/or to its ability to afford payment for extortion demands (Cimpanu 2020). Specifically, the literature on the motivations of cybercriminals indicates that firm disclosure about counter-breach initiatives and investments attracts their attention for *more frequent attacks* seeking profit, fame, or challenge to exploit targets that they know enough about (Havakhor et al. 2020). In addition, cyber insurance may lead to complacency in that the insureds' incentive to invest in self-protection measures is reduced following the purchase of the insurance (Eling and Schnell 2016).

Thus, the relationship between cyber insurance and the timeliness of breach announcement and frequency of cyber breaches are empirical questions and lead to the second hypothesis:

**Hypothesis 2a** (H2a): *The disclosure of cyber insurance is not associated with the timelier announcement of a data breach.*

**Hypothesis 2b** (H2b): *The disclosure of cyber insurance is not associated with the timelier resolution of a data breach.*

**Hypothesis 2c** (H2c): *The disclosure of cyber insurance is not associated with a lower frequency of data breaches.*

## 4.3 Research design

### 4.3.1 Data source

To extract cyber insurance disclosure, the study focuses on "Item 1A. Risk Factors" because the SEC encourages firms to disclose their cyber insurance in this section. Specifically, the SEC states that appropriate disclosures of cybersecurity risks and cyber incidents may include "a description of relevant insurance coverage" (SEC 2011) and "costs associated with maintaining cybersecurity protections, including, if applicable, insurance coverage relating to cybersecurity incidents or payments to service providers" (SEC 2018). To better understand the key terms that firms use to disclose their cyber insurance, the study manually examines 300 randomly selected "Item 1A. Risk Factors" sections from the sample. The search reveals that firms (1) disclose information about their cyber insurance policy in relation to cybersecurity risks and cyber incidents, (2) generally indicate that such coverage is not adequate to cover the losses in case of cyber incidents, and (3) do not disclose negation of maintaining such policy (unlike environmental insurance disclosure). Appendix A provides examples of cyber insurance disclosure.

Firms use a range of key terms to refer to cyber insurance: "cybersecurity insurance", "cybersecurity breach insurance", "cyber insurance", "cyber coverage", "cyber liability insurance", "cyber-risk insurance policy", "information security risk insurance coverage", "insurance against the risk of cyberattacks", and "insurance designed to provide coverage for cyber risks". To capture cyber insurance disclosure, the study performs a proximity search on "insurance" and (cyber, data breach, data security, security breach, security incident, system

failure, information security risk).[30] This search strategy returns all "Item 1A. Risk Factors" that contain any of these phrases within 50-words of the word insurance.[31] In addition, the phrase "cyber coverage" does not contain the term "insurance", thus the study also search for the phrase "cyber coverage" separately. As an additional validation step that the search accurately captures and extracts cyber insurance, the study randomly selects and manually analyzes 400 of "Item 1A. Risk Factors" sections. This step reveals that Type I and Type II error rates are less than 5%. Finally, in comparison to search strategies of recent studies (Florackis et al. 2023; Jamilov et al. 2021; Smith et al. 2019), the search strategy is more inclusive, thus providing further comfort that it captures most, if not all, disclosures about cyber insurance. There are 13,893 **"**Item 1A. Risk Factors" sections that disclose the cyber insurance policy.

The study focuses on a sample period from 2010 to 2021 because 2010 is the year preceding the SEC 2011 cybersecurity guidance and stops on 2021 as that where the Advisen data ends. Moreover, prior research highlights the increase of (1) firms' cybersecurity risk disclosure following the SEC guidance (SEC 2011; 2018), (2) cybersecurity risks, and (3) cybersecurity awareness (Berkman et al. 2018; Florackis et al. 2023).[32] Using the CIK, and the fiscal year, the study links the results of the search with financial data from Compustat, corporate governance data from BoardEx, and cybersecurity breach events from Advisen Ltd.[33] Advisen Ltd is "the foremost provider of data, media, and technology solutions for the commercial property and casualty

[30] The term "cyber" captures all variations of cyber, including cyber, cybersecurity, cyber-security, cyberattack(s), cyber-attack, etc.
[31] The 50 words distance is similar to the one used in Jamilov et al. (2021).
[32] For example, Florakis et al. (2020) indicates that by 2012, more than 66% of U.S. firms disclose their cybersecurity risks in their 10-K filings compared to 39% in 2010, and by 2018, the disclosure of cybersecurity risks in "Item 1A. Risk Factors" section increased to 90% of U.S. firms. Moreover, the sample is limited to firms that have an "Item 1A. Risk Factors" section, excluding small firms that are not required to provide such information and also firms that disclose the "Item 1A. Risk Factors" section by reference in a separate document.
[33] Many studies examine Advisen dataset including Romanosky (2016), and Hogan et al. (2020). For more information: https://www.advisenltd.com/about/.

insurance market". Table 1 presents the sample selection for the main sample (Panel A) and breach sample (Panel B).

…….. [Insert Table 1 about here] ……...……...

### 4.3.2 Models and variables measurement

To address the question of whether the joint probability of having cyber insurance and disclosing it ($CYBER\_INSURANCE_{i,t}$) is associated with the likelihood of a breach ($BREACH_{i,t+1}$) (Hypothesis 1), the study estimates the following multivariate logistic regression.

$$
\begin{aligned}
Prob\,(BREACH_{i,t+1} = 1) \\
&= \beta_0 + \boldsymbol{\beta_1 CYBER\_INSURANCE_{i,t}} + \beta_2 FIRM\_SIZE_{i,t} + \beta_3 FIRM\_AGE_{i,t} \\
&+ \beta_4 ROA_{i,t} + \beta_5 LEVERAGE_{i,t} + \beta_6 LOSS_{i,t} + \beta_7 R\&D\_EXPENDITURE_{i,t} \\
&+ \beta_8 CASH\_HOLDINGS_{i,t} + \beta_9 PAST\_BREACH_{i,t} + \beta_{10} CIO\_ROLE_{i,t} \\
&+ \beta_{11} CYBER\_RISK_{i,t} + \beta_{12} COMPLIANCE\_COMMITTEE_{i,t} \\
&+ \beta_{13} RISK\_COMMITTEE_{i,t} + \beta_{14} TECHNOLOGY\_COMMITTEE_{i,t} \\
&+ \lambda_1 YearFixedEffects + \lambda_2 IndustryFixedEffects + \varepsilon_{i,t} \qquad (1)
\end{aligned}
$$

The dependent variable is $BREACH_{i,t+1}$, an indicator variable equal to one if firm *i* reports a cyber breach in year *t+1*, and zero otherwise. The independent variable of interest is $CYBER\_INSURANCE_{i,t}$, which is an indicator variable taking the value of one if firm *i* reports having cyber insurance in "Item 1A. Risk Factors" of its 10-K in year *t*, and zero otherwise. Thus, the coefficient of interest is $\beta_1$, where a positive (negative) coefficient indicates that disclosure of cyber insurance increases (decreases) the likelihood of a cyber breach. The model includes firm's characteristics measures of size ($FIRM\_SIZE_{i,t}$), leverage ($LEVERAGE_{i,t}$), loss ($LOSS_{i,t}$), profitability ($ROA_{i,t}$), research and development ($R\&D\_EXPENDITURE_{i,t}$), and age ($FIRM\_AGE_{i,t}$), as larger profitable older firms with intellectual property and less financial constraints are more attractive breach targets (Benaroch and Chernobai 2017; Ettredge et al. 2018; Higgs et al. 2016). To control for additional factors that likely explain breaches, the study controls for whether the firm has previously reported a breach ($PAST\_BREACH_{i,t}$).

Furthermore, presence of technology, risk, or compliance board-level committees may be associated with the likelihood of a cyber breach (Higgs et al. 2016; Smith et al. 2021). Thus, indicator variables identifying firms with such committees are incorporated in the model including: ($COMPLIANCE\_COMMITTEE_{i,t}$), ($RISK\_COMMITTEE_{i,t}$), and ($TECHNOLOGY\_COMMITTEE_{i,t}$). Moreover, the study controls for cash reserve ($CASH\_HOLDINGS_{i,t}$), as firms may use increased cash reserves as an efficient way to cover consequential cyber incident damages (i.e., indirect costs such as reputational costs) that are not covered by cyber insurance (Boasiako and Keefe 2021). Additionally, the study controls for the presence of chief information officer (CIO) and/or similar role ($CIO\_ROLE_{i,t}$) as presence of such a role indicates a higher level of a firm's development of cybersecurity management reporting structure (Tsen et al. 2020) and associates with reduced data breaches (Haislip et al. 2021).

At the industry level, the study includes a control for firms operating in high cyber risk industries ($CYBER\_RISK_{i,t}$), as cybersecurity breach cost, frequency, and severity differ based on industry affiliation.[34] Following Ashraf (2021), $CYBER\_RISK_{i,t}$ is defined as one if firm *i* belongs to one of these industries: financial services, healthcare, retail, manufacturing, or information and communications, and zero otherwise. The model incorporates year and industry fixed effects. Appendix B summarizes all variable definitions.

The decision to purchase cyber insurance is not random as firms that are likely to purchase cyber insurance may also be more likely to be targets of a breach. To address such potential endogeneity, the study uses a propensity score matching approach following Lawrence et al. (2011). Specifically, the study estimates the probability of purchasing cyber insurance, then

[34] A recent report by IBM (2021) indicates that healthcare organizations experienced the highest average cost of a data breach, while financial industry suffers the greatest number of cyber incidents.

matches with firms with no cyber insurance using predicted value within a 3 percent of maximum distance. Thus, the study develops a cyber insurance prediction model including variables that explain the decision to purchase and disclose cyber insurance policy as well as independent control variables from the main breach determinant model (Equation 1). The model is as follow:

$$
\begin{aligned}
&CYBER\_INSURANCE_{i,t+1} \\
&\quad = \gamma_0 + \gamma_1 FIRM\_SIZE_{i,t} + \gamma_2 FIRM\_AGE_{i,t} + \gamma_3 ROA_{i,t} + \gamma_4 LEVERAGE_{i,t} + \gamma_5 LOSS_{i,t} \\
&\quad + \gamma_5 CASH\_HOLDINGS_{i,t} + \gamma_6 R\&D\_EXPENDITURE_{i,t} + \gamma_7 COMPLEXITY_{i,t} \\
&\quad + \gamma_8 HIGH\_TECH_{i,t} + \gamma_9 PAST\_BREACH_{i,t} + \gamma_{10} CIO\_ROLE_{i,t} \\
&\quad + \gamma_{11} TECHNOLOGY\_COMMITTEE_{i,t} + \gamma_{12} RISK\_COMMITTEE_{i,t} \\
&\quad + \gamma_{13} COMPLIANCE\_COMMITTEE_{i,t} + \gamma_{14} PEER\_CYBER\_INSURANCE_{i,t} \\
&\quad + \gamma_{15} PEER\_NUM_{i,t} + \gamma_{16} CYBER\_RISK_{i,t} + \lambda_1 YearFixedEffects \\
&\quad + \lambda_2 IndustryFixedEffects + \varepsilon_{i,t} \qquad (2)
\end{aligned}
$$

The variable high-intensity IT ($HIGH\_TECH_{i,t}$) in the model captures the situation that firms operating in high-intensity IT processes face relatively high secondary losses from cyber events, hence they are more likely to purchase cyber insurance policy to hedge high proportion of their cyber risks (Bandyopadhyay et al. 2009). In addition, the study controls for a firm's business and geographic complexity ($COMPLEXITY_{i,t}$) on the assumption that more complex firms are more exposed to cyber breaches and therefore are more likely to purchase cyber insurance. Appendix B defines all variables.

To mitigate the potential for endogeneity from omitted variables, the study uses a two-stage least squares (2SLS) instrumental variable approach. As instruments, the study uses percentage (number) of peer disclosure of cyber insurance ($PEER\_CYBER\_INSURANCE_{i,t}$ and $PEER\_NUM_{i,t}$). Prior studies document the impact of peer effects in various corporate decisions (Ashraf 2021; Cho and Muslu 2021; Seo 2021). Thus, firms could purchase cyber insurance to simply mimic the practice of their industry peers. Particularly, when more industry peers manage cyber risk by transferring it to a third party, a firm will be more likely to have and disclose cyber insurance.

To address the self-selection problem, the study follows a Heckman (1979) two-stage approach and estimate Equation (2) using a Probit model in the first stage, and then include the inverse Mills ratio (IMR) from this stage as an additional control variable in Equation (1). Cyber insurance model (first stage) includes two new exclusion variables namely percentage (number) of local cyber insurance peers ($L\_PEER\_CYBER\_INSURANCE_{i,t}$ and $L\_PEER\_NUM_{i,t}$), which the study expects to be associated with the likelihood of purchasing and disclosing cyber insurance but not with the likelihood of a breach. Choosing these instrumental variables is based on assumption that firms are more likely to commit to cyber insurance when resources are available and easy to access. Thus, if the area a firm resides in has such resources, then the firm is more likely to manage cyber risk via insurance.

The study uses the following model to examine the impact of cyber insurance in the event of a breach:

$$
\begin{aligned}
&BREACH\_CONSEQUENCE_{i,t} \\
&\quad = \beta_0 + \boldsymbol{\beta_1 CYBER\_INSURANCE_{i,t}} + \beta_2 FIRM\_SIZE_{i,t} + \beta_3 ROA_{i,t} \\
&\quad + \beta_4 LEVERAGE_{i,t} + \beta_5 LOSS_{i,t} + \beta_6 R\&D\_EXPENDITURE_{i,t} + \beta_7 CASH\_HOLDINGS_{i,t} \\
&\quad + \beta_8 FIRM\_AGE_{i,t} + \beta_9 PAST\_BREACH_{i,t} + \beta_{10} CYBER\_RISK_{i,t} \\
&\quad + \beta_{11} BREACH\_TYPE_{i,t} + \beta_{12} INFORAMTION\_TYPE_{i,t} + \beta_{13} ACTORS_{i,t} \\
&\quad + \beta_{14} SEVERITY_{i,t} + \beta_{15} SOURCE_{i,t} + \lambda_1 YearFixedEffects \\
&\quad + \lambda_2 IndustryFixedEffects + \varepsilon_{i,t} \qquad (3)
\end{aligned}
$$

The study examines the association between cyber insurance and three breach consequences ($BREACH\_CONSEQUENCE_{i,t}$); namely, timeliness of breach announcement ($DISCLOSURE\_TIMELINESS_{i,t}$), timeliness of breach resolution ($RESOLUTION\_TIMELINESS_{i,t}$), and breach frequency ($BREACH\_FREQUENCY_{i,t}$). The model incorporates a set of cyber breach characteristics namely breach type ($BREACH\_TYPE_{i,t}$), types of data, assets, or information that has been compromised ($INFORMATION\_TYPE_{i,t}$), whether the breach event is initiated by internal or external actors ($ACTORS_{i,t}$), number of records

lost ($SEVERITY_{i,t}$), and the source of breach ($SOURCE_{i,t}$). Similar to equation (1), the study controls for the firm and industry characteristics. Appendix B summarizes all variable definitions.

**4.3.3 Descriptive statistics and correlations**

Table 2 shows summary statistics for the main and breach samples. For the main sample, Panel A shows 40 percent of firm-year observations report breach events, and 26 percent disclose cyber insurance in Item 1A of 10-K filings. Statistics for control variables are generally consistent with prior literature. About 28 percent of observations report the existence of CIO role, 82 percent operate in high cyber risk industries, three percent experience prior breach, and 18 percent have a risk committee. For breach sample, Panel B shows, on average, it takes firms 108.8 days to disclose the breach and 96.54 days to resolve and contain the breach. Furthermore, on average the sample experienced 9.67 breach recurrence.

…….. [Insert Table 2 about here] ……...……...

Figure 1 presents cyber insurance disclosure and the number of breaches per year. The figure exhibits a positive time trend for cyber insurance disclosure, especially after 2011, when the SEC issued the first cybersecurity disclosure guidance. The increase in cyber insurance is notable, increasing from 6 (1 percent) in 2011 to 1347 (20 percent) in 2020. Similarly, the number of disclosed breaches shows a positive time trend until 2017. Thus, time trend of cyber insurance disclosure aligns with the number of breaches, reflecting that increasing concerns over risk of breaches (from 36 in 2011 to 1119 in 2020) are pushing firms to transfer such risk to a third party.

…….. [Insert Figure 1 about here] ……...……...

Figure 2 presents the cyber insurance disclosure across the Fama-French 12 industries. The figure shows clear cross-industry differences, where cyber insurance disclosure is more marked in Finance, Business Equipment and Software, and Healthcare sectors. These industries rely heavily

on information technology systems and store large amounts of data, which makes them more vulnerable to breaches.[35] Specifically, 89 percent of the total number of breaches occur in these industries, hence possibly leading to more cyber insurance disclosures, where 77 percent of total cyber insurance disclosures are by such industries. Firms in more "traditional" industries such as Chemical; Consumer Durables; and Consumer Nondurables exhibit fewer breaches (0.01 percent of the total number of breaches) and correspondingly lower (2 percent) cyber insurance disclosures.

…….. [Insert Figure 2 about here] ……..……...

Table 3 provides Pearson correlations for the full (Panel A) and the breach (Panel B) samples. For the full sample, Panel (A) shows *CYBER_INSURANCE* is significantly positively correlated with the *BREACH* (coefficient of 0.04). This result indicates that cyber insurance disclosure attracts unwanted attention of hackers. There are significant positive correlations between *BREACH* and *FIRM_SIZE, FIRM_AGE*, *CYBER_RISK*, and negative correlations with *LOSS* and *LEVERAGE*.

For the breach sample, Panel (B) shows while *DISCLOSURE_TIMELINESS* (coefficient of 0.02) is positively correlated with *CYBER_INSURANCE, RESOLUTION_TIMELINESS* (coefficient of -0.05) and *BREACH_FREQUENCY* (coefficient of -0.07) are negatively correlated with the *CYBER_INSURANCE*. Moreover, firm characteristics such as *PAST_BREACH* and *CYBER_RISK*, (*FIRM_AGE, R&D_EXPENDITURE,* and *CASH_HOLDINGS*) are significantly positively (negatively) correlated with *CYBER_INSURANCE.* The study explores the relation between cyber insurance disclosure and probability of breaches, as well as the relation between cyber insurance disclosure and breach consequences further in subsequent multivariate analyses.

[35] Financial industry is also characterized by higher quality enterprise risk management (ERM) (Baxter et al. 2013), which may be a factor their higher purchase of cyber insurance.

…….. [Insert Table 3 about here] ……...……...

### 4.4 Analysis and results

#### 4.4.1 Main results

Table 4 presents the regression results for hypothesis (1). The multivariate models (2) and (3) are reasonable and provide sufficient level of predictive ability as the area under the *ROC* curve for the models is greater than 0.90. Model (1) reports results without controls and fixed effects; Model (2) reports results with controls; and Model (3) reports results with controls and fixed effects. *CYBER_INSURANCE* is positively associated with the likelihood of a breach across the three models. Focusing on Model (3), the coefficient of *CYBER_INSURANCE* is positive and statically significant (0.412, $p$-value ≤ 0.001). Disclosing cyber insurance increases the likelihood of a breach event by 51 percent, which may be due to disclosure attracting unwanted attention from hackers, or firms with such insurance are paying less attention to safeguard against cyber breaches, or both. With respect to control variables, firm characteristics of size, profitability, leverage, cash reserve, and R&D expenditure are positively related with the likelihood of a breach and are consistent with prior literature (Kamiya et al. 2021). Furthermore, firms operating in cyber risk industries are more likely to be targets of a breach (1.343, $p$-value ≤ 0.001). Similar to Kamiya et al. (2021), the study reports a negative coefficient estimate for *RISK_COMMITTEE* (-0.325, $p$-value ≤ 0.001), and opposite to Higgs et al. (2016), the study reports a negative coefficient estimate for *TECHNOLOGY_COMMITTEE* (-0.376, $p$-value ≤ 0.001).

…….. [Insert Table 4 about here] ……...……...

Based on Figure 1, cyber insurance disclosure and number of breaches are more pronounced in finance industries, thus the study examines the model using a sub-sample that excludes financial firms and a sub-sample of only financial firms. Models (4) and (5) of Table 4

present the results of hypothesis (1) based on these sub-samples. The results indicate that *CYBER_INSURANCE* is positively associated with the likelihood of a breach for both nonfinancial (0.520, *p*-value ≤ 0.001) and financial firms (0.358, *p*-value ≤ 0.001). Furthermore, the signs and significance levels of control variables are similar for both sub-samples except for *LOSS*, *R&D_EXPENDITURE*, *CASH_HOLDINGS*, *COMPLIANCE_COMMITTEE*, and *TECHNOLOGY_COMMITTEE*. Furthermore, having a *TECHNOLOGY_COMMITTEE*, *CASH_HOLDINGS*, and *R&D_EXPENDITURE* are significantly associated with *BREACH* events for non-financial firms (-0.722, *p*-value ≤ 0.001; 0.761, *p*-value ≤ 0.001; 3.315, *p*-value ≤ 0.001, respectively), while reporting *LOSS* and having *COMPLIANCE_COMMITTEE* are significantly related with a *BREACH* for financial firms (-0.757, *p*-value ≤ 0.001; 0.327, *p*-value ≤ 0.05, respectively).

### 4.4.2 Breach consequences

Table 5 presents results for the association between *CYBER_INSURANCE* and breach consequences in terms of *DISCLOSURE_TIMELINESS*, *RESOLUTION_TIMELINESS*, and *BREACH_FREQUENCY*. The empirical model used is Equation (3). Models (1) to (3) report the results for the association between *CYBER_INSURANCE* and *DISCLOSURE_TIMELINESS* (hypothesis a2). Model (3) shows that *CYBER_INSURANCE* is positively related with *DISCLOSURE_TIMELINESS* (0.109, *p*-values ≤ 0.001), where *CYBER_INSURANCE* increases, on average, the time firms take to disclose the breach by 1.12 days. This finding supports the notion that the cyber insurance providers take time to investigate and provide the affected firm access to their expert counseling and legal expertise. About control variables, *FIRM_AGE,* and breach characteristics in terms of *SEVERITY, BREACH_TYPE* involving privacy, and type of information loss (*INFORMATION_TYPE*) are positively related with *DISCLOSURE_TIMELINESS*. However,

*R&D_EXPENDITURE, CASH_HOLDINGS,* breach *ACTORS,* and client hardware as breach *SOURCE* are negatively related with *DISCLOSURE_TIMELINESS.*

Models (4) to (6) of Table (5) report the results for the association between *CYBER_INSURANCE* and *RESOLUTION_TIMELINESS* (hypothesis b2). Focusing on Model (6), *CYBER_INSURANCE* is significant and negatively (-0.337, *p*-values ≤ 0.001) related with the *RESOLUTION_TIMELINESS,* indicating that cyber insurance reduces on average the time firms take to resolve and contain the breach event by 1.40 days. This finding highlights that *CYBER_INSURANCE* benefits firms by providing access to the insurance firm's expertise in handling the aftermath of a breach in a more timely manner. About control variables, the coefficients of *FIRM_SIZE, FIRM_AGE, LEVERAGE*, and *LOSS* are positive, while *R&D_EXPENDITURE* is negative. Breach characteristics in terms of number of records lost (*SEVERITY)*, whether the lost information in these records is personal or corporate (*INFORMATION_TYPE*), and the type of the breach (data or privacy) (*BREACH_TYPE)* are positively related with *RESOLUTION_TIMELINESS.* Nevertheless, *SOURCE* of the breach (being client hardware; server, cloud, Web; and telecommunication) are negatively related with *RESOLUTION_TIMELINESS.*

…….. [Insert Table 5 about here] ……...……...

Models (7) to (9) of Table (5) report the results for the association between *CYBER_INSURANCE* and *BREACH_FREQUENCY* (Hypothesis c2). Focusing on Model (9), *CYBER_INSURANCE* is significant and positively (0.099, *p*-values ≤ 0.001) associated with *BREACH_FREQUENCY.* This finding validates the main result in Table 4, where firms disclosing *CYBER_INSURANCE* expose themselves and become a target of a future *BREACH.* Firm characteristics in terms of *FIRM_SIZE, FIRM_AGE, PROFITABILITY, R&D_EXPENDITURE*

and (*CASH_HOLDINGS*, *PAST_BREACH,* and operating in high *CYBER_RISK* industries) are positively (negatively) related with recurrence of the breach. About breach characteristics, *ACTORS, BREACH_TYPE* (involving data and privacy)*, and INFORMATION_TYPE* are positively related with *BREACH_FREQUENCY,* while *SOURCE* of breach involving client hardware and privacy law are negatively related with *BREACH_FREQUENCY.*

### 4.4.3 Additional tests

*4.4.3.1 Risk section length, high-tech, tangibility, and internal control weaknesses*

A firm with higher cybersecurity risk provides lengthier and more comprehensive cybersecurity risk disclosure, describing risks and their potential consequences, and/or mitigating initiatives put in place by the firm to reduce such impact and therefore disclosing its cyber insurance. Campbell et al. (2014) demonstrate that a firm's level of risk exposure determines the amount of disclosure it devotes to handle such risk. In addition, Filzen (2015) indicates that the more disclosure of risks, the higher the likelihood of a negative event. Accordingly, it is possible that the probability of a breach and cyber insurance disclosure is driven by the length of risk disclosure. Controlling for the length of Item 1A. Risk Factors in the analysis (*RISK_SECTION_LENGTH*), Table (6) shows the main inferences remain unchanged across the full sample (Model 1).

Firms operating in high-intensity IT settings may face relatively high probability of a breach event due to their more reliance on technology. The main inference remains the same after controlling for *HIGH_TECH* (Model 2 of Table 6). Moreover, prior research documents that firm tangibility as one of the most robust predictors of cybersecurity risk exposure. For example, Kamiya et al. (2021) and Florackis et al. (2023) find that firms with higher asset tangibility are

more likely to be targets of a cyberattack. Thus, controlling for firms' assets tangibility structure (*TANGIBILITY*), Model (3) of Table 6 shows that the main inferences stay the same.

Finally, flaws in firms' internal control systems may expose them to breaches (Lawrence et. al 2018). Thus, the study includes an indicator variable for firms' internal control weakness ($ICW$) in Equation (1). The main inference stays the same (Model 4 of Table 6).

…….. [Insert Table 6 about here] ……...……...

*4.4.3.2 Breach consequences across industries and CEO power*

Panel A of Table 7 estimates the impact of cyber insurance on breach consequences controlling for whether breaches are more likely in certain industries. Based on number of observations across industries, the regression includes only five industries (Fama-French 12) (namely, *BUSINESS_EQUIPMENT_AND_SOFTWARE*; *WHOLESALE_AND_RETAIL*; *HEALTHCARE*; *FINANCE*; and *MANUFACTURING*) and uses manufacturing as a reference group.[36] Model (1) shows none of the industries is significantly related with *DISCLOSURE_TIMELINESS.* However, the main inference of *CYBER_INSURANCE* being negatively related with *DISCLOSURE_TIMELINESS* remains the same. Model (2) reports that *BUSINESS_EQUIPMENT_AND_SOFTWARE* and *HEALTHCARE* industries are positively related with *RESOLUTION_TIMELINESS* (1.044, $p$-values $\leq$ 0.05; 1.070, $p$-values $\leq$ 0.1, respectively). This finding demonstrates the better capacity of these industries to resolve breaches. In Model (3), all industries are positively related with *BREACH_FREQUENCY,* thus all industry types are similarly impacted vis-a-vis the recurrence of the breach.

[36] The study excludes industries with less than 5% of the total observations.

The association between firms' disclosure of cyber insurance and breach consequences may be confounded by the presence of a powerful CEO. Thus, the study controls for the CEO power (*CEO_POWER*) and Panel B of Table 7 shows that the main results stay the same.

…….. [Insert Table 7 about here] ……...……...

*4.4.3.3 Cyber insurance coverage disclosed after a breach event*

Firms that implemented risk reduction measures may disclose such internal information related to their risk assessment (Gordon et al. 2010). Given that cyber insurance disclosure is voluntary, it is possible that a firm may have such coverage even if it is not explicitly mentioned in their annual report. A possible way to mitigate the impact of such issue confounding the main results, the study examines breached firms that disclosed their cyber insurance post a breach event, in compliance with the SEC requirement that firms disclose insurance information as part of a cyber incident disclosure. The data indicates that about 2 percent of breached firms disclose their cyber insurance post a breach event. Excluding these firms in Equation (1), the untabulated results support the main findings of positive association between the disclosure of cyber insurance and probability of a breach.

**4.4.4 Endogeneity and sample selection bias**

This section summarizes the results of endogeneity and sample selection bias tests including the use of the propensity score matching (PSM), two-stage least squares (2SLS) with instrumental variables, and Heckman two-stage model.

For PSM, each cyber insurance firm-year is matched with one control firm-year based on firm size, age, profitability, industry sector (Fama-French 12), and fiscal year.[37] Table 8 reports the difference in means of a PSM sample based on whether a firm discloses cyber insurance or

[37] Similar to Kamiya et al. (2021), matching based on fiscal year induces an "artificial" cyberattack on the matched firms.

not. Overall, the means of all variables are significantly different between firms that disclose cyber insurance versus those that do not. Moreover, the univariate analysis reveals that cyber insurance disclosing firms are, on average, smaller, older, have less cash holdings, and are more likely to have a prior breach.

…….. [Insert Table 8 about here] ……...……...

Model (1) of Table 9 presents the PSM regression results. The result shows a sufficient level of predictive ability at 95 percent. The coefficient of *CYBER_INSURANCE* is positive (2.728, *p*-values ≤ 0.001), indicating that cyber insurance is associated with the likelihood of a future breach, which suggests that study's findings do not suffer from observable sample selection bias. About control variables results (unreported), their signs and significance levels are similar to the main sample results, except for *LEVERAGE, LOSS,* and *R&D_EXPENDITURE*. The study finds significant positive coefficients for *LOSS* and no significant level for *LEVERAGE* and *R&D_EXPENDITURE*.

To mitigate the potential for endogeneity from omitted variables, Models (2) and (3) of Table 9 summarize the results of using the 2SLS regression. Model (2) reports the first-stage regression results based on Equation (2), where *CYBER_INSURANCE* is the dependent variable and the percentage (number) of cyber insurance peers (*PEER_CYBER_INSURANCE* and *PEER _NUM*) as instrumental variables. The coefficient of instruments *PEER_CYBER_INSURANCE* and *PEER_NUM* are significant (7.691, *p*-values ≤ 0.001; 0.138, *p*-values ≤ 0.001, respectively), indicating that industry peers' practices are critical factors when firms are deciding to transfer cyber risk via insurance. Model (3) shows the second-stage regression results of *CYBER_INSURANCE* and probability of a future *BREACH*. The coefficient of

*CYBER_INSURANCE* is positive (0.738, *p*-values ≤ 0.001), even when controlling for endogeneity.

To address the potential self-selection bias, Models (4) and (5) of Table 9 summarize the results of using the Heckman (1979) two-stage approach. Model (4) reports the first stage results based on Equation (2), using the percentage (number) of local peers' cyber insurance (*L_PEER_CYBER_INSURANCE* and *L_PEER_NUM*) as new instrumental variables. The coefficients of these instruments are positive and significant, thus signifying that availability of local resources are important factors when firms are deciding to transfer cyber risk via insurance. Model (5) reports the second-stage regression results. The coefficient of *CYBER_INSURANCE* is positive (2.642, *p*-value ≤ 0.001).[38] Moreover, the coefficient of *IMR* is significant, suggesting that findings are not driven by sample selection bias.

Overall, findings reported in Table 9 provide robust evidence of the positive association between cyber insurance disclosing firms' and the likelihood of being breached relative to firms that do not disclose.

…….. [Insert Table 9 about here] ……...……...

**4.5 Conclusion**

This study examines whether firms disclosing their cyber insurance are more likely to be target of a data breach, and how effective having cyber insurance is if a firm is breached. Using textual analysis of cyber insurance disclosure in "Item 1A. Risk Factors" section of 10-K filings for the period 2010-2021, the study finds that disclosing cyber insurance increases the likelihood of a firm being a target of a future breach event. This finding may indicate either that disclosure

[38] The results of Variance Inflation Factors (VIF) indicate no multicollinearity issue, where VIFs for all test variables are below the conventional cut-off of 10 (Feng et al. 2009).

of cyber insurance is attracting unwanted attention from hackers, or that firms with such insurance are paying less attention to safeguard against data breaches (or both).

In the event of an actual data breach, effectiveness of cyber insurance depends on the nature of the breach consequence. In the case of the breach disclosure timeliness, having cyber insurance increases the time firms take to disclose such breach. However, in the case of the breach resolution timeliness, the results show that holding cyber insurance reduces the time firms take to resolve and contain the breach. This finding highlights that cyber insurance benefits firms by providing access to their insurance providers' expertise in handling the aftermath of a breach in a more timely manner. Finally, in the case of breach recurrence, the study finds a positive relation between cyber insurance and breach frequency, supporting the main finding that disclosing cyber insurance exposes firms to become targets of future breaches.

The current study contributes to the disclosure and cybersecurity literature as it examines both pre- and post-impacts of cyber insurance as effective risk management tools. The findings in this study should be of interest to academics, practitioners, and regulators as they offer timely and relevant evidence on the interaction between data breaches and cyber insurance on one hand, and cyber insurance and breach consequences on the other hand, especially that disclosure of cyber insurance is voluntary. The first limitation of this study is that it does not consider the actual economic cost of a breach due to limited availability of such data, which may be a fruitful future research venue if such data can be obtained. Furthermore, the study attempted to mitigate the issue of identification of firms that have and do not disclose their cyber insurance, yet other approaches may be used for further confirmation of our results. Finally, the impact of hackers sharing information on the dark web or their other sophisticated activities on the breach status of a firm, is a standing limitation of this study and a possible future research direction.

## 4.6 References, figures, tables, and appendices

### References


Aguilar, L. A. (2014, June). Boards of directors, corporate governance and cyber-risks: Sharpening the focus. In Cyber Risks and the Boardroom conference, New York Stock Exchange.

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

Anderson R., Barton C., Bohme R., Clayton R., Eeten M., & Levi, M. (2012). Measuring the cost of cybercrime. In: Proceedings of the 11th Workshop on the Economics of Information Security (WEIS'12). Available at https://cseweb.ucsd.edu/~savage/papers/WEIS2012.pdf

Ashraf, M. (2021). The role of peer events in corporate governance: Evidence from data breaches. *The Accounting Review, 97*(2), 1-24.

Bandyopadhyay, T., Mookerjee, V. S., & Rao, R. C. (2009). Why IT managers don't go for cyber-insurance products. *Communications of the ACM*, *52*(11), 68-73.

Baxter, R., Bedard, J. C., Hoitash, R., & Yezegel, A. (2013). Enterprise risk management program quality: Determinants, value relevance, and the financial crisis. *Contemporary Accounting Research*, *30*(4), 1264-1295.

Benaroch, M., & Chernobai, A. (2017). Operational IT failures, IT value-destruction, and board-level IT governance changes. *MIS Quarterly*, *41*(3), 729–762.

Berkman, H., Jona, J., Lee, G., & Soderstrom, N. (2018). Cybersecurity awareness and market valuations. *Journal of Accounting and Public Policy*, *37*(6), 508-526.

Biener, C., Eling, M., & Wirfs, J. H. (2015). Insurability of cyber risk: An empirical analysis. *The Geneva Papers on Risk and Insurance-Issues and Practice*, *40*(1), 131-158.

Biros, D., Havakhor, T., & Zhang, T. (2019). Does cybersecurity slow down digitization? A natural experiment of security breach notification laws. Working paper [ssrn3382000].

Boasiako, K. A., & Keefe, M. O. C. (2021). Data breaches and corporate liquidity management. *European Financial Management*, *27*(3), 528-551.

Bodin, L. D., Gordon, L. A., Loeb, M. P., & Wang, A. (2018). Cybersecurity insurance and risk-sharing. *Journal of Accounting and Public Policy*, *37*(6), 527-544.

Bonner, L. (2012). Cyber risk: How the 2011 Sony data breach and the need for cyber risk insurance policies should direct the federal response to rising data breaches. *Journal of Law & Policy*, *40*, 257-277.

Boyer, M. M. (2014). Directors' and officers' insurance and shareholder protection. *Journal of Financial Perspectives*, *2*(1).

Boyer, M. M. (2020). Cyber insurance demand, supply, contracts and cases. *The Geneva Papers on Risk and Insurance-Issues and Practice*, *45*(4), 559-563.

Campbell, J. L., Chen, H., Dhaliwal, D. S., Lu, H. M., & Steele, L. B. (2014). The information content of mandatory risk factor disclosures in corporate filings. *Review of Accounting Studies*, *19*(1), 396-455.

Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: Empirical evidence from the stock market. *Journal of Computer Security*, *11*(3), 431-448.

Cheong, A., Yoon, K., Cho, S., & No, W. G. (2021). Classifying the contents of cybersecurity risk disclosure through textual analysis and factor analysis. *Journal of Information Systems*, *35*(2), 179-194.

Cho, H., & Muslu, V. (2021). How do firms change investments based on MD&A disclosures of peer firms? *The Accounting Review*, *96*(2), 177-204.

Cimpanu, C. (2020, September 10). *Ransomware accounted for 41% of all cyber insurance claims in H1 2020*. ZDNet. https://www.zdnet.com/article/ransomware-accounts-to-41-of-all-cyber-insurance-claims/

Cohen, J., Krishnamoorthy, G., & Wright, A. (2017). Enterprise risk management and the financial reporting process: The experiences of audit committee members, CFOs, and external auditors. *Contemporary Accounting Research*, 34(2), 1178-1209.

Coker, J. (2020, December 23). *Cyber Insurance Market Expected to Surge in 2021*. *Infosecurity Magazine*. https://www.infosecurity-magazine.com/news/cyber-insurance-market-surge-2021/

Crosignani, M., Macchiavelli, M., & Silva, A. F. (2023). Pirates without borders: The propagation of cyberattacks through firms' supply chains. *Journal of Financial Economics*, *147*(2), 432-448.

Department of Homeland Security (DHS). 2017. Cybersecurity Insurance. https://www.dhs.gov/cybersecurity-insurance (Accessed June 16, 2022).

Eisenbach, T. M., Kovner, A., & Lee, M. J. (2022). Cyber risk and the US financial system: A pre-mortem analysis. *Journal of Financial Economics*, *145*(3), 802-826.

Eling, M., & Schnell, W. (2016). What do we know about cyber risk and cyber risk insurance? *Journal of Risk Finance*, *17* (5), 474-491.

Eling, M., & Wirfs, J. (2019). What are the actual costs of cyber risk events? *European Journal of Operational Research*, *272*(3), 1109-1119.

Ettredge, M., Guo, F., & Li, Y. (2018). Trade secrets and cyber security breaches. *Journal of Accounting and Public Policy*, *37*(6), 564-585.

Feng, M., Li, C., & McVay, S. (2009). Internal control and management guidance. *Journal of Accounting and Economics*, *48*(2-3), 190-209.

Filzen, J. J. (2015). The information content of risk factor disclosures in quarterly reports. *Accounting Horizons*, *29*(4), 887-916.

Florackis C., Louca C., Michaely R., & Weber M. (2023). Cybersecurity risk. *The Review of Financial Studies*, *36*(1), 351-407.

Foerderer, J., & Schuetz, S. W. (2022). Data breach announcements and stock market reactions: A matter of timing?. *Management Science*, *68*(10), 7298-7322.

Francis B., Hu. W., Shohfi D. T. (2021). Ex-Intrusion corporate cyber-risk: Evidence from Internet Protocol Networks. *Journal of Operational Risk*, *16*(3).

Frank, M., Maksymov, E., Peecher, M., & Reffett, A. (2021). Beyond risk shifting: The knowledge-transferring role of audit liability insurers. *Contemporary Accounting Research*, *38*(3), 2224-2263.

Freifeld, K. (2014). U.S. companies allowed to delay disclosure of data breaches. *Reuters*. Available at: https://www.reuters.com/article/us-target-data-notification-idUSBREA0F1LO20140116 (Accessed October 19, 2022)

Gal-Or, E., & Ghose, A. (2005). The economic incentives for sharing security information. *Information Systems Research*, *16*(2), 186-208.

Gao, L., Calderon, T. G., & Tang, F. (2020). Public companies' cybersecurity risk disclosures. *International Journal of Accounting Information Systems*, *38*, 100468.

Gordon, L. A., Loeb, M. P., & Sohail, T. (2003). A framework for using insurance for cyber-risk management. *Communications of the ACM*, *46*(3), 81-85.

Gordon, L. A., Loeb, M. P., & Sohail, T. (2010). Market value of voluntary disclosures concerning information security. *MIS Quarterly*, 567-594.

Government Accountability Office (GAO). (2021, May 20). *Cyber Insurance: Insurers and Policyholders Face Challenges in an Evolving Market* GAO-21-477. U.S. Government Accountability Office. Available at https://www.gao.gov/products/gao-21-477 (Accessed August 13, 2021)

Greenwald, J. (2021, August 31). *Cyber disclosures attract SEC's attention*. Business Insurance. Available at: https://www.businessinsurance.com/article/20210831/NEWS06/912344206/Cyber-disclosures-attract-SEC%E2%80%99s-attention (Accessed April 5, 2022)

Haislip, J., Kolev, K., Pinsker, R., & Steffen, T. (2019). The economic cost of cybersecurity breaches: A broad-based analysis. *In Workshop on the Economics of Information Security (WEIS),* 1-37.

Haislip, J., Lim, J. H., & Pinsker, R. (2021). The impact of executives' IT expertise on reported data security breaches. *Information Systems Research, 32*(2), 318-334.

Hampton, C., Sutton, S. G., Arnold, V., & Khazanchi, D. (2021). Cyber supply chain risk management: Toward an understanding of the antecedents to demand for assurance. *Journal of Information Systems*, *35*(2), 37-60.

Havakhor, T., Rahman, M. S., & Zhang, T. (2020). Cybersecurity investments and the cost of capital. Working paper [SSRN 3553470].

He, C., HuangFu, J., Kohlbeck, M. J., & Wang, L. (2020). The impact of customer's reported cybersecurity breaches on key supplier's relationship-specific investments and relationship duration. Working paper [SSRN 3544245].

Heckman, J. J. (1979). Sample selection bias as a specification error. *Econometrica: Journal of the Econometric Society*, 153-161.

Héroux, S., & Fortin, A. (2020). Cybersecurity disclosure by the companies on the S&P/TSX 60 index. *Accounting Perspectives*, *19*(2), 73-100.

Higgs, J. L., Pinsker, R. E., Smith, T. J., & Young, G. R. (2016). The relationship between board-level technology committees and reported security breaches. *Journal of Information Systems*, *30*(3), 79-98.

Hobson, A., & Adams, I. (2020). California dreams about cyber insurance, and federal lawmakers should pay attention. Available at: https://thehill.com/opinion/cybersecurity/486427-california-dreams-about-cyber-insurance-federal-lawmakers (Accessed May 15, 2021)

Hogan, K. M., Olson, G. T., & Angelina, M. (2020). A comprehensive analysis of cyber data breaches and their resulting effects on shareholder wealth. Working paper [SSRN 3589701].

Huang, H. H., & Wang, C. (2021). Do banks price firms' data breaches? *The Accounting Review*, 96(3), 261-286.

IBM. (2020). Cost of a data breach report 2020. Available at https://www.ibm.com /downloads /cas/RZAX14GX

IBM. (2021). Cost of a data breach report 2021. Available at: https://www.ibm.com /security/ data-breach

Jackson, S., Vanteeva, N., & Fearon, C. (2019). An investigation of the impact of data breach severity on the readability of mandatory data breach notification letters: Evidence from US firms. *Journal of the Association for Information Science and Technology*, *70*(11), 1277-1289.

Jamilov, R., Rey, H., & Tahoun, A. (2021). The anatomy of cyber risk. Working paper [No. w28906], National Bureau of Economic Research.
Janvrin, D. J., & Wang, T. D. (2022). Linking cybersecurity and accounting: An event, impact, response framework linking cybersecurity and accounting. *Accounting Horizons*, *36*(4), 67-112.
Jensen, M. C., & Meckling, W. H. (1976). Theory of the firm: Managerial behavior, agency costs and ownership structure. *Journal of Financial Economics*, *3*(4), 305-360.
Jiang, W., Legoria, J., Reichelt, K., & Walton, S. (2021). Firm use of cybersecurity risk disclosure. *Journal of Information Systems, 36*(1), 151-180.
Jorgensen, B. N., & Kirschenheiter, M. T. (2003). Discretionary risk disclosures. *The Accounting Review, 78*(2), 449-469.
Kabir, U. Y., Ezekekwu, E., Bhuyan, S. S., Mahmood, A., & Dobalian, A. (2020). Trends and best practices in health care cybersecurity insurance policy. *Journal of Healthcare Risk Management*, *40*(2), 10-14.
Kamiya, S., Kang, J. K., Kim, J., Milidonis, A., & Stulz, R. M. (2021). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics*, *139*(3), 719-749.
Kasznik, R., & Lev, B. (1995). To warn or not to warn: Management disclosures in the face of an earnings surprise. *The Accounting Review*, 113-134.
Klein, A., Manini, R., & Shi, Y. (2022). Across the pond: How US firms' boards of directors adapted to the passage of the General Data Protection Regulation. *Contemporary Accounting Research, 39*(1), 199-233.
Koijen, R. S., & Yogo, M. (2022). New perspectives on insurance. *The Review of Financial Studies*, *35*(12), 5275-5286.
Kopp, E., Kaffenberger, L., & Wilson, C. (2017). Cyber risk, market failures, and financial stability. *International Monetary Fund*. https://ssrn.com/abstract=3024075.
Kshetri, N. (2020). The evolution of cyber-insurance industry and market: An institutional analysis. *Telecommunications Policy*, *44*(8), 102007.
Lawrence, A., Minutti-Meza, M., & Vyas, D. (2018). Is operational control risk informative of financial reporting deficiencies? *Auditing: A Journal of Practice & Theory*, *37*(1), 139-165.
Lawrence, A., Minutti-Meza, M., & Zhang, P. (2011). Can Big 4 versus non-Big 4 differences in audit-quality proxies be attributed to client characteristics? *The Accounting Review*, *86*(1), 259-286.
Lennox, C. S., Francis, J. R., & Wang, Z. (2012). Selection models in accounting research. *The Accounting Review*, *87*(2), 589-616.
Li, H., No, W. G., & Boritz, J. E. (2020). Are external auditors concerned about cyber incidents? Evidence from audit fees. *Auditing: A Journal of Practice & Theory, 39*(1), 151-171.
Lieberman, M. (2017, December 8). *Mind The Trust Gap: How Companies Can Retain Customers After A Security Breach*. Forbes. Available at: https://www.forbes.com/sites/forbestechcouncil/2017/12/08/mind-the-trust-gap-how-companies-can-retain-customers-after-a-security-breach/?sh=7e2e4c616c95 (Accessed April 2021)
Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data privacy: Effects on customer and firm performance. *Journal of Marketing*, *81*(1), 36-58.
Maurer, C., Kim, K., Kim, D., & Kappelman, L. A. (2021). Cybersecurity: Is it worse than we think? *Communications of the ACM*, *64*(2), 28-30.

Mittel, M. (2020). Navigating the cyber-insurance landscape to protect MSPs and their clients. *Computer Fraud & Security*, *2020*(1), 12-14.

Mukhopadhyay, A., Chatterjee, S., Bagchi, K. K., Kirs, P. J., & Shukla, G. K. (2019). Cyber risk assessment and mitigation (CRAM) framework using logit and probit models for cyber insurance. *Information Systems Frontiers*, *21*(5), 997-1018.

Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A., & Sadhukhan, S. K. (2013). Cyber-risk decision models: To insure IT or not? *Decision Support Systems*, *56*, 11-26.

National Institute for Standards and Technology (NIST). (2018). Framework for improving the critical infrastructure cybersecurity. Available at: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (Accessed April 2021)

Ogbanufe, O., Kim, D. J., & Jones, M. C. (2021). Informing cybersecurity strategic commitment through top management perceptions: The role of institutional pressures. *Information & Management*, *58*(7), 103507.

Palsson, K., Gudmundsson, S., & Shetty, S. (2020). Analysis of the impact of cyber events for cyber insurance. *The Geneva Papers on Risk and Insurance-Issues and Practice*, *45*(4), 564-579.

Panda, S., Farao, A., Panaousis, E., & Xenakis, C. (2021). Cyber-Insurance: Past, present and future. *Encyclopedia of Cryptography, Security and Privacy,* https://doi.org/10.1007/978-3-642-27739-9_1624-1

PwC. (2018). Global state of information security survey 2018. Available at: https://www.pwc.co.uk/issues/cyber-security-services/insights/global-state-of-information-security-survey.html (Accessed February 2022)

PwC. (2021). Insurance 2020 & beyond: Reaping the dividends of cyber resilience. Available at: https://www.pwc.com/gx/en/insurance/publications/assets/reaping-dividends-cyber-resilience.pdf (Accessed February 2022)

Romanosky, S. (2016). Examining the costs and causes of cyber incidents. *Journal of Cybersecurity, 2*(2), 121-135.

Romanosky, S., Ablon, L., Kuehn, A., & Jones, T. (2019). Content analysis of cyber insurance policies: How do carriers price cyber risk? *Journal of Cybersecurity*, *5*(1), tyz002.

Sabbagh, D. (2021, January 24). *Insurers "funding organized crime" by paying ransomware claims*. The Guardian. Available at: https://www.theguardian.com/technology/2021/jan/24/insurers-funding-organised-by-paying-ransomware-claims (Accessed February 2022)

Schoenfeld, J. (2022). Cyber risk and voluntary Service Organization Control (SOC) audits. *Review of Accounting Studies*, 1-41.

Securities and Exchange Commission (SEC). (2011). Cf disclosure guidance: Topic no. 2. Available at: Https://www.Sec.Gov/divisions/corpfin/guidance/cfguidance-topic2.Htm.

Securities and Exchange Commission (SEC). (2018). Commission statement and guidance on public company cybersecurity disclosures (February 26). Release Nos. 33-10459; 34-82746. Washington, DC: SEC.

Seo, H. (2021). Peer effects in corporate disclosure decisions. *Journal of Accounting and Economics*, *71*(1), 101364.

Shackelford, S. J. (2012). Should your firm invest in cyber risk insurance? *Business Horizons*, *55*(4), 349-356.

Shumsky, T. (2016). Corporate judgment call: When to disclose you've been hacked. *The Wall Street Journal*. (September 19). Available at: https://www.wsj.com/articles/corporate-judgment-call-when-to-disclose-youve-been-hacked-1474320689

Skinner, D. J. (1997). Earnings disclosures and stockholder lawsuits. *Journal of Accounting and Economics*, *23*(3), 249-282.

Smith, T. J., Higgs, J. L., & Pinsker, R. E. (2019). Do auditors price breach risk in their audit fees? *Journal of Information Systems*, *33*(2), 177-204.

Smith, T., Tadesse, A. F., & Vincent, N. E. (2021). The impact of CIO characteristics on data breaches. *International Journal of Accounting Information Systems*, *43*, 100532.

Sonnemaker, T. (2019). *Facing Inevitable Data Breaches and New Privacy Laws, Companies Shift Focus to Response*. Medill Reports Chicago. Available at: https://news.medill.northwestern.edu/chicago/facing-inevitable-data-breaches-and-new-privacylaws-companies-shift-focus-to-response/ (Accessed September 10, 2021)

Stine, K., Quinn, S., Witte, G., Scarfone, K., & Gardner, R. (2020). Integrating cybersecurity and enterprise risk management (ERM). (No. NIST Internal or Interagency Report (NISTIR), 8286). National Institute of Standards and Technology.

Stoller, D. (2020). Cyber insurance purchases will surge with California privacy law. Bloomberg law. Available at https://news.bloomberglaw.com/privacy-and-data-security/cyber-insurance-purchases-will-surge-with-california-privacy-lawc (Accessed May 7, 2021)

Swinhoe, D. (2022). *The biggest data breach fines, penalties, and settlements so far*. CSO Online. Available at: https://www.csoonline.com/article/3410278/the-biggest-data-breach-fines-penalties-and-settlements-so-far.html (Accessed June 12, 2022)

Talesh, S. A. (2018). Data breach, privacy, and cyber insurance: How insurance companies act as "compliance managers" for businesses. *Law & Social Inquiry*, *43*(2), 417-440.

Tsen, E., Ko, R. K., & Slapničar, S. (2020). Organizational cyber resilience and its influence on cyber-attack outcomes: An exploratory study of 1,145 publicized attacks. *Working paper* [SSRN:3735636].

Verrecchia, R. E. (1983). Discretionary disclosure. *Journal of Accounting and Economics*, *5*, 179-194.

Verrecchia, R. E. (2001). Essays on disclosure. *Journal of Accounting and Economics*, *32*(1-3), 97-180.

Walton, S., Wheeler, P., Zhang, Y., & Zhao, X. (2020). An integrative review and analysis of cybersecurity research: Current state and future directions. *Journal of Information Systems*, ISYS-19.

Wang, T., Kannan, K. N., & Ulmer, J. R. (2013). The association between the disclosure and the realization of information security risk factors. *Information Systems Research*, *24*(2), 201-218.

Figure 1 Cyber Insurance Disclosure by Year

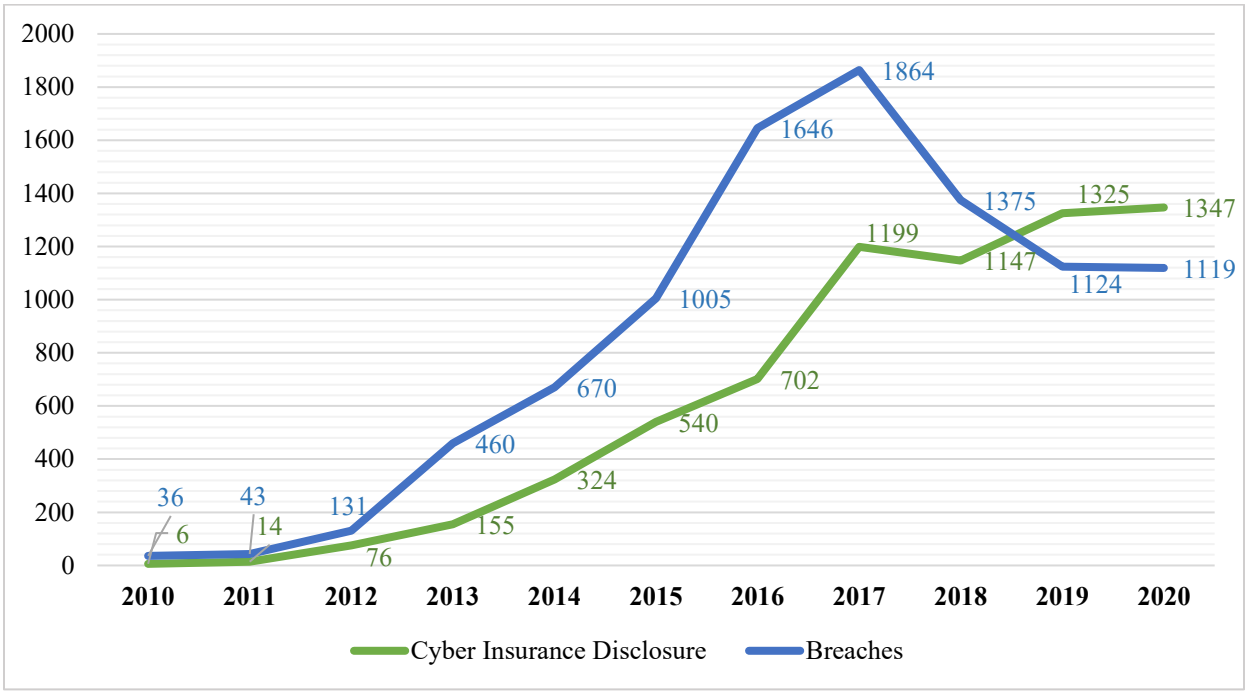


Figure 1 displays cyber insurance disclosure and the number of Advisen actual breaches by year.

Figure 2 Cyber Insurance Disclosure Across Industry Sectors

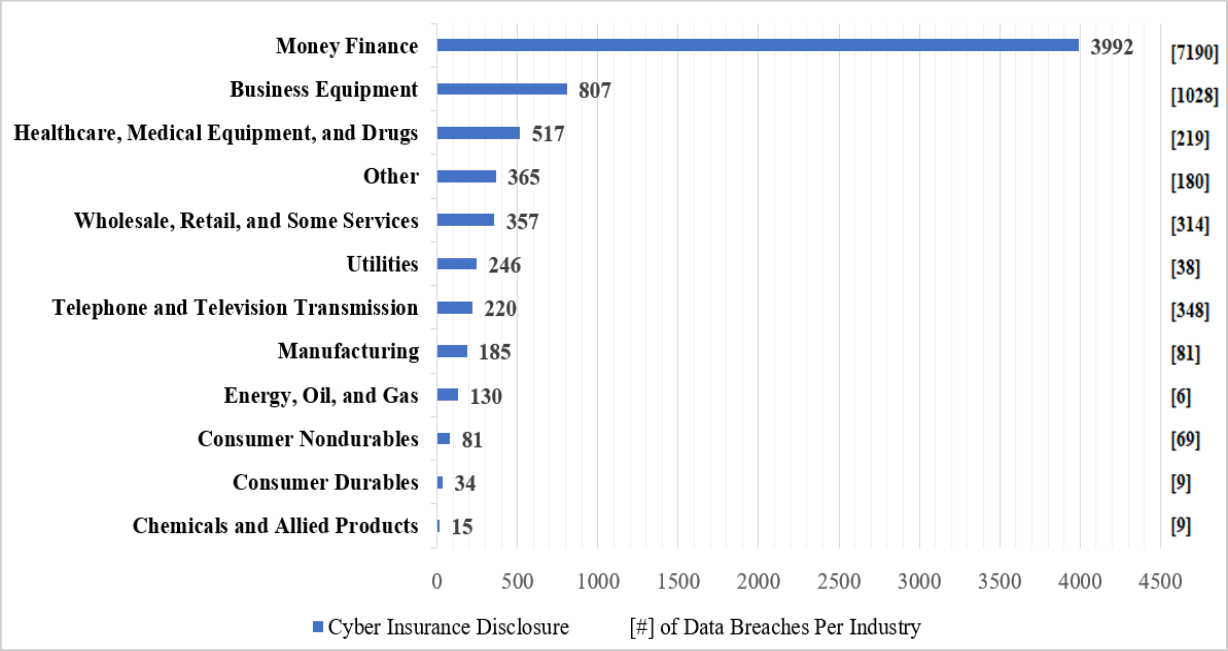


Figure 2 displays cyber insurance disclosure and the number of breaches by industry sector. Firms are classified into Fama-French 12 industries.

TABLE 1 Sample Selection

| **Panel A: Main Sample Selection** | **Firm-year Obs.** | **No. of Firms** |
|---|---|---|
| Firm Item 1A Risk Factors section of 10-K filings from 2010-2021 | 107,914 | 5,131 |
| Less: Firms in insurance industries (SIC codes 6311–6499) | 1,633 | 92 |
| Less: Firms without necessary data from Compustat and BoardEx | 80,414 | 2,473 |
| Less: Observations removed due to lag calculation | 2,610 | 567 |
| **Total firms' observation sample** | **23,257** | **1,999** |

| **Panel B: Breach Sample Selection** | **Firm-year Obs.** | **No. of Firms** |
|---|---|---|
| Total number of breach events from 2009-2021(Advisen) | 174,447 | 67,803 |
| Less: Observations of government, not for profit, and private organizations | 133,210 | 57,340 |
| Less: Observations of non-U.S. public companies | 5,792 | 2,724 |
| Less: Observations with missing CIK | 24,687 | 5,787 |
| Less: Observations with missing data from Compustat and BoardEx | 1,257 | 1,536 |
| Less: Observations removed due to lag calculation | 188 | 47 |
| **Total sample of breach events attributed to U.S. public companies** | **9,303** | **369** |

Table 1 presents study sample selection. Panel A provides the main sample construction. Panel B provides breach events sample construction.

TABLE 2 Descriptive Statistics

| **Panel A:** Main Sample | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Variable | N | Mean | SD | P25 | Median | P75 | Min | Max |
| *BREACH* | 23,257 | 0.40 | 0.49 | 0.00 | 0.00 | 1.00 | 0.00 | 1.00 |
| *CYBER_INSURANCE* | 23,257 | 0.26 | 0.44 | 0.00 | 0.00 | 1.00 | 0.00 | 1.00 |
| *FIRM_SIZE* | 23,257 | 9.72 | 2.93 | 7.61 | 9.19 | 11.92 | -2.16 | 15.20 |
| *FIRM_AGE* | 23,257 | 31.51 | 18.97 | 16.00 | 26.00 | 46.00 | 1.00 | 72.00 |
| *ROA* | 23,257 | 0.04 | 0.17 | 0.00 | 0.02 | 0.10 | -7.35 | 1.75 |
| *LEVERAGE* | 23,257 | 0.26 | 0.34 | 0.10 | 0.20 | 0.36 | 0.00 | 24.77 |
| *LOSS* | 23,257 | 0.14 | 0.35 | 0.00 | 0.00 | 0.00 | 0.00 | 1.00 |
| *R&D_EXPENDITURE* | 23,257 | 0.02 | 0.07 | 0.00 | 0.00 | 0.00 | -0.01 | 2.24 |
| *CASH_HOLDINGS* | 23,257 | 0.11 | 0.16 | 0.00 | 0.03 | 0.16 | 0.00 | 0.99 |
| *PAST_BREACH* | 23,257 | 0.03 | 0.16 | 0.00 | 0.00 | 0.00 | 0.00 | 1.00 |
| *CIO_ROLE* | 23,257 | 0.28 | 0.45 | 0.00 | 0.00 | 1.00 | 0.00 | 1.00 |
| *CYBER_RISK* | 23,257 | 0.82 | 0.39 | 1.00 | 1.00 | 1.00 | 0.00 | 1.00 |
| *COMPLIANCE_COMMITTEE* | 23,257 | 0.04 | 0.21 | 0.00 | 0.00 | 0.00 | 0.00 | 1.00 |
| *RISK_COMMITTEE* | 23,257 | 0.18 | 0.38 | 0.00 | 0.00 | 0.00 | 0.00 | 1.00 |
| *TECHNOLOGY_COMMITTEE* | 23,257 | 0.05 | 0.22 | 0.00 | 0.00 | 0.00 | 0.00 | 1.00 |
| **Panel B:** Breach Sample | | | | | | | | |
| *SEVERITY* | 8036 | 2.27 | 3.53 | 0.00 | 0.00 | 4.08 | 0.00 | 21.51 |
| *ACTOR* | 9211 | 0.65 | 0.48 | 0.00 | 1.00 | 1.00 | 0.00 | 1.00 |
| *INFORMATION_TYPE* | 9241 | 0.95 | 0.22 | 1.00 | 1.00 | 1.00 | 0.00 | 1.00 |
| *DISCLOSURE_TIMELINESS* | 7900 | 4.69 | 1.87 | 3.40 | 4.99 | 6.01 | 0.00 | 8.54 |
| *RESOLUTION_TIMELINESS* | 2286 | 4.57 | 1.90 | 3.33 | 4.63 | 5.98 | 0.00 | 8.35 |
| *BREACH_FREQUENCY* | 9303 | 2.16 | 1.06 | 1.39 | 2.40 | 3.00 | 0.00 | 3.89 |

Table 2 reports descriptive statistics for the full and breach samples. Panel A reports 23,257 observations for the main sample that are available on the SEC's EDGAR, Compustat, BoardEx, and Advisen databases. The variables are pooled across fiscal years 2010–2021. Panel B reports descriptive statistics for the breach characteristics sample. All variables are defined in detail in Appendix B.

TABLE 3 Correlation Matrix

**Panel (A): Full Sample**

| | *Variables* | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** | **12** | **13** | **14** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **1** | *BREACH* | | | | | | | | | | | | | | |
| **2** | *CYBER_INSURANCE* | **0.04** | | | | | | | | | | | | | |
| **3** | *FIRM_SIZE* | **0.71** | 0.01 | | | | | | | | | | | | |
| **4** | *FIRM_AGE* | **0.28** | **-0.06** | **0.53** | | | | | | | | | | | |
| **5** | *ROA* | **0.02** | 0.01 | **0.07** | **0.06** | | | | | | | | | | |
| **6** | *LEVERAGE* | **-0.06** | 0.00 | **-0.09** | **-0.02** | **-0.27** | | | | | | | | | |
| **7** | *LOSS* | **-0.24** | **-0.02** | **-0.39** | **-0.19** | **-0.27** | **0.12** | | | | | | | | |
| **8** | *R&D_EXPENDITURE* | **-0.11** | **-0.03** | **-0.31** | **-0.16** | **-0.33** | **0.09** | **0.34** | | | | | | | |
| **9** | *CASH_HOLDINGS* | **-0.02** | **-0.07** | **-0.21** | **-0.12** | **-0.06** | **-0.11** | **0.27** | **0.56** | | | | | | |
| **10** | *PAST_BREACH* | **0.04** | **0.06** | 0.00 | 0.00 | **0.05** | **0.02** | 0.00 | 0.01 | **0.03** | | | | | |
| **11** | *CIO_ROLE* | **0.37** | **-0.09** | **0.36** | **0.28** | **0.02** | -0.01 | **-0.05** | 0.01 | **0.09** | **0.02** | | | | |
| **12** | *CYBER_RISK* | **0.31** | **0.03** | **0.26** | **0.03** | **-0.05** | **-0.19** | **-0.11** | **0.12** | **0.13** | 0.00 | **0.15** | | | |
| **13** | *COMPLIANCE_COMMITTEE* | **0.02** | **0.04** | **0.02** | **0.02** | **0.03** | **0.03** | **-0.02** | **-0.04** | **-0.07** | 0.00 | **0.03** | **0.04** | | |
| **14** | *RISK_COMMITTEE* | **0.24** | 0.00 | **0.36** | **0.16** | **-0.07** | **-0.07** | **-0.15** | **-0.13** | **-0.11** | **-0.04** | **0.09** | **0.18** | **-0.10** | |
| **15** | *TECHNOLOGY_COMMITTEE* | **0.03** | **0.02** | **0.04** | **0.07** | **-0.03** | -0.01 | 0.01 | **0.06** | **0.03** | 0.01 | **0.05** | **0.07** | **-0.05** | **-0.11** |

**Panel (B): Breach Sample**

| | *Variables* | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** | **12** | **13** | **14** | **15** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **1** | *CYBER_INSURANCE* | | | | | | | | | | | | | | | |
| **2** | *FIRM_SIZE* | 0.01 | | | | | | | | | | | | | | |
| **3** | *FIRM_AGE* | **-0.06** | **0.53** | | | | | | | | | | | | | |
| **4** | *ROA* | 0.01 | **0.07** | **0.06** | | | | | | | | | | | | |
| **5** | *LEVERAGE* | 0.00 | **-0.09** | **-0.02** | **-0.27** | | | | | | | | | | | |
| **6** | *LOSS* | **-0.02** | **-0.39** | **-0.19** | **-0.27** | **0.12** | | | | | | | | | | |
| **7** | *R&D_EXPENDITURE* | **-0.03** | **-0.31** | **-0.16** | **-0.33** | **0.09** | **0.34** | | | | | | | | | |
| **8** | *CASH_HOLDINGS* | **-0.07** | **-0.21** | **-0.12** | **-0.06** | **-0.11** | **0.27** | **0.56** | | | | | | | | |
| **9** | *PAST_BREACH* | **0.06** | 0.00 | 0.00 | **0.05** | **0.02** | 0.00 | 0.01 | **0.03** | | | | | | | |
| **10** | *CYBER_RISK* | **0.03** | **0.26** | **0.03** | **-0.05** | **-0.19** | **-0.11** | **0.12** | **0.13** | 0.00 | | | | | | |
| **11** | *SEVERITY* | **-0.03** | **-0.25** | **-0.20** | **0.28** | **-0.11** | **0.09** | **0.26** | **0.27** | **0.06** | **-0.13** | | | | | |
| **12** | *ACTOR* | **0.05** | **0.19** | **0.16** | **-0.20** | **0.17** | **-0.08** | **-0.27** | **-0.24** | **-0.04** | **0.12** | **-0.41** | | | | |
| **13** | *INFORMATION_TYPE* | 0.00 | **0.03** | **-0.02** | **-0.06** | **0.04** | -0.01 | **-0.06** | **-0.09** | **-0.05** | **0.02** | **-0.13** | **0.22** | | | |
| **14** | *DISCLOSURE_TIMELINESS* | **0.02** | **0.08** | **0.07** | **-0.13** | **0.18** | **-0.04** | **-0.18** | **-0.18** | **-0.04** | **0.05** | **-0.26** | **0.33** | **0.12** | | |

| | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **15** | *RESOLUTION_TIMELINESS* | **-0.05** | **0.18** | **0.16** | **-0.19** | **0.10** | 0.00 | **-0.22** | **-0.08** | **-0.04** | 0.02 | **-0.20** | **0.29** | **0.10** | **0.83** | |
| **16** | *BREACH_FREQUENCY* | **-0.07** | **0.41** | **0.22** | **-0.07** | **-0.17** | **-0.24** | **0.06** | **0.06** | **-0.18** | **0.30** | **-0.13** | **0.14** | **0.14** | **0.11** | **0.12** |

Table 3 reports Pearson correlation coefficients for the main sample variables (Panel A) and breach sample (Panel B). See Appendix B for variables definitions. Values in bold indicate statistical significance at 1 percent or better.

TABLE 4 Predicting Breaches with Firm Disclosure of Cyber Insurance

| | *Dependent Variable = $BREACH_{t+1}$ (indicator)* | | | | |
|---|---|---|---|---|---|
| | Full Sample | | | Non-Financial Sample | Financial Sample |
| | (1) | (2) | (3) | (4) | (5) |
| *CYBER_INSURANCE* | 0.174*** | 0.427*** | 0.412*** | 0.520*** | 0.358*** |
| | (5.775) | (8.981) | (8.126) | (6.765) | (4.859) |
| *FIRM_SIZE* | | 1.124*** | 1.142*** | 0.813*** | 1.437*** |
| | | (69.783) | (66.035) | (32.508) | (52.460) |
| *FIRM_AGE* | | -0.034*** | -0.031*** | -0.022*** | -0.04*** |
| | | (-23.472) | (-19.317) | (-10.184) | (-15.984) |
| *ROA* | | 3.333*** | 2.951*** | 2.928*** | 6.013*** |
| | | (12.086) | (9.495) | (7.609) | (9.118) |
| *LEVERAGE* | | 0.68*** | 0.685*** | -0.719*** | 1.785*** |
| | | (6.421) | (7.220) | (-3.897) | (10.277) |
| *LOSS* | | -0.094 | -0.062 | 0.026 | -0.757*** |
| | | (-1.052) | (-0.656) | (0.233) | (-3.326) |
| *R&D_EXPENDITURE* | | 4.756*** | 4.943*** | 3.315*** | -6.257 |
| | | (8.416) | (7.546) | (5.091) | (-0.341) |
| *CASH_HOLDINGS* | | 1.478*** | 1.087*** | 0.761*** | -0.635 |
| | | (7.344) | (5.103) | (2.920) | (-1.470) |
| *CYBER_RISK* | | 1.24*** | 1.343*** | 0.964*** | 1.651*** |
| | | (16.554) | (13.123) | (7.519) | (9.491) |
| *PAST_BREACH* | | 0.749*** | 0.566*** | 0.701*** | 0.406* |
| | | (6.583) | (4.900) | (5.494) | (1.789) |
| *CIO_ROLE* | | 1.013*** | 0.958*** | 0.411*** | 1.444*** |
| | | (19.436) | (17.223) | (5.438) | (15.563) |
| *COMPLIANCE_COMMITTEE* | | 0.078 | 0.168 | 0.231 | 0.327** |
| | | (0.794) | (1.614) | (1.560) | (2.019) |
| *RISK_COMMITTEE* | | -0.287*** | -0.325*** | -0.768*** | -0.321*** |
| | | (-4.665) | (-5.083) | (-3.605) | (-4.143) |
| *TECHNOLOGY_COMMITTEE* | | -0.422*** | -0.376*** | -0.722*** | -0.200 |
| | | (-4.547) | (-3.833) | (-4.863) | (-1.346) |
| Year Fixed Effects | No | No | Yes | Yes | Yes |
| Industry Fixed Effects | No | No | Yes | Yes | No |
| # Observations | 23257 | 23257 | 23257 | 9715 | 13542 |
| Pseudo $R^2$ | 0.001 | 0.537 | 0.552 | 0.365 | 0.607 |
| Area Under ROC | 0.517 | 0.943 | 0.950 | 0.899 | 0.968 |

Table 4 shows the association between firm disclosure of cyber insurance and probability of a future breach for different samples. The sample consists of 23,257 firm-year observations over the period 2010 to 2021. The dependent variable in each regression is probability of $BREACH_{t+1}$, an indicator variable that takes the value of one if a firm experiences a breach in a year t+1 and zero otherwise. The independent variable of interest in each regression is *CYBER_INSURANCE*, defined as one if firm *i* discloses cyber insurance in "Item 1A. Risk Factors" of 10-K filings in year *t,* or zero otherwise. Models (1)-(3) present regression results for the full sample, where Model (1) presents results without controls and fixed effects, Model (2) provides results with controls, and Model (3) reports results with controls and fixed effects. Models (4) and (5) present regression results for subsamples of non-financial (Model 4) and financial (Model 5) firms. The empirical model used in this table is Equation (1). All variables are defined in detail in Appendix B. The regression includes an intercept but is not tabulated for parsimony. The *t-statistics* are in parentheses and *, **, and *** indicate significance at the 10%, 5% and 1% levels, respectively.

TABLE 5 Impact of Cyber Insurance on Breach Consequences

| *Dependent Variable* | *DISCLOSURE_TIMELINESS* | | | *RESOLUTION_TIMELINESS* | | | *BREACH_FREQUENCY* | | |
|---|---|---|---|---|---|---|---|---|---|
| | Model (1) | Model (2) | Model (3) | Model (4) | Model (5) | Model (6) | Model (7) | Model (8) | Model (9) |
| *CYBER_INSURANCE* | 0.098** | 0.060 | 0.109*** | -0.194** | -0.281*** | -0.337*** | -0.159*** | 0.101*** | 0.099*** |
| | (2.111) | (1.588) | (2.732) | (-2.179) | (-3.232) | (-3.624) | (-6.511) | (4.546) | (4.452) |
| *FIRM_SIZE* | | -0.011 | -0.014 | | 0.078*** | 0.065* | | 0.205*** | 0.183*** |
| | | (-0.918) | (-1.024) | | (2.754) | (1.950) | | (27.765) | (23.712) |
| *FIRM_AGE* | | 0.003*** | 0.003** | | 0.010*** | 0.009*** | | -0.001 | 0.002** |
| | | (2.679) | (2.550) | | (3.613) | (3.195) | | (-1.572) | (2.517) |
| *ROA* | | -0.750*** | 0.067 | | -0.258 | 1.160 | | 1.51*** | 1.718*** |
| | | (-2.998) | (0.217) | | (-0.346) | (1.276) | | (10.530) | (10.318) |
| *LEVERAGE* | | 0.118 | -0.048 | | 0.842*** | 0.897*** | | -0.222*** | 0.078 |
| | | (1.120) | (-0.433) | | (3.044) | (3.002) | | (-3.444) | (1.219) |
| *LOSS* | | -0.242** | -0.081 | | 0.438** | 0.609*** | | -0.691*** | -0.686*** |
| | | (-2.453) | (-0.794) | | (2.180) | (2.787) | | (-12.179) | (-12.204) |
| *R&D_EXPENDITURE* | | -2.232*** | -1.176** | | -4.186*** | -9.283*** | | 5.231*** | 3.694*** |
| | | (-5.044) | (-2.280) | | (-3.083) | (-5.666) | | (19.890) | (12.760) |
| *CASH_HOLDINGS* | | -0.54*** | -0.533*** | | 0.567 | 0.311 | | 0.007 | -0.356*** |
| | | (-3.355) | (-3.187) | | (1.474) | (0.803) | | (0.074) | (-3.785) |
| *PAST_BREACH* | | -0.041 | 0.000 | | -0.021 | 0.038 | | -0.613*** | -0.558*** |
| | | (-0.432) | (-0.003) | | (-0.098) | (0.183) | | (-10.815) | (-10.411) |
| *CYBER_RISK* | | -0.228** | -0.020 | | -0.579** | -0.419 | | 0.870*** | 0.704*** |
| | | (-2.215) | (-0.136) | | (-2.414) | (-0.985) | | (14.390) | (8.699) |
| *SEVERITY* | | 0.022*** | 0.019*** | | 0.021* | 0.034*** | | -0.013*** | -0.004 |
| | | (3.926) | (3.404) | | (1.877) | (2.836) | | (-4.020) | (-1.234) |
| *ACTORS* | | -0.303*** | -0.289*** | | -0.268* | -0.075 | | 0.074** | 0.074** |
| | | (-5.422) | (-5.143) | | (-1.760) | (-0.488) | | (2.434) | (2.527) |
| *BREACH_TYPE (DATA)* | | -0.316*** | -0.337*** | | 0.579*** | 0.754*** | | 0.262*** | 0.170*** |
| | | (-4.078) | (-4.321) | | (3.513) | (4.440) | | (5.724) | (3.895) |
| *BREACH_TYPE (PRIVACY)* | | 1.505*** | 1.519*** | | 2.254*** | 2.204*** | | 0.391*** | 0.316*** |
| | | (9.270) | (9.338) | | (6.156) | (6.074) | | (3.986) | (3.383) |
| *INFORMATION_TYPE* | | 0.942*** | 1.073*** | | 1.279*** | 1.647*** | | 0.296** | 0.358*** |
| | | (4.642) | (5.303) | | (2.801) | (3.632) | | (2.341) | (2.992) |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| *SOURCE (Client Hardware)* | | -0.555** | -0.603** | | -1.199** | -0.917* | | -0.326** | -0.261** |
| | | (-2.332) | (-2.543) | | (-2.387) | (-1.856) | | (-2.403) | (-2.037) |
| *SOURCE (Server, Cloud, Web)* | | -0.233 | -0.226 | | -1.256*** | -1.161** | | 0.022 | 0.017 |
| | | (-0.981) | (-0.953) | | (-2.617) | (-2.458) | | (0.163) | (0.134) |
| *SOURCE (Telecommunication)* | | 0.322 | 0.254 | | -1.050* | -0.939* | | -0.023 | -0.058 |
| | | (1.161) | (0.920) | | (-1.813) | (-1.648) | | (-0.145) | (-0.380) |
| *SOURCE (Privacy Law)* | | 0.390 | 0.377 | | -0.904 | -0.703 | | -0.304* | -0.388** |
| | | (1.376) | (1.331) | | (-1.475) | (-1.163) | | (-1.840) | (-2.480) |
| Year Fixed Effects | No | No | Yes | No | No | Yes | No | No | Yes |
| Industry Fixed Effects | No | No | Yes | No | No | Yes | No | No | Yes |
| # Observations | 7900 | 6622 | 6622 | 2286 | 1955 | 1955 | 9303 | 7835 | 7835 |
| $R^2$ | 0.001 | 0.439 | 0.454 | 0.002 | 0.287 | 0.333 | 0.005 | 0.330 | 0.412 |

Table 5 estimates the impact of cyber insurance on breach consequences. The dependent variable in Models (1) to (3) is *DISCLOSURE_TIMELINESS*, defined as natural log of time firm *i* takes to announce breach in year *t*; dependent variable in Models (4) to (6) is *RESOLUTION_TIMELINESS*, defined as natural log of time firm *i* takes to resolve the breach in year *t*; and dependent variable in Model (7) to (9) is *BREACH_FREQUENCY*, defined as natural log of number of breach events for firm *i* in year *t*. The sample runs from 2010 to 2021. The empirical model used in this table is Equation (3). The regression includes an intercept but is not tabulated for parsimony. Appendix B contains details of these variables. The *t-statistics* are in parentheses and ***, **, and * indicate significance at the 0.01, 0.05, and 0.10 levels, respectively.

TABLE 6 Predicting Breaches with Firm Disclosure of Cyber Insurance Controlling for Risk Section Length, High-Tech, Tangibility, and Internal Control Weaknesses

| | *Dependent Variable = $BREACH_{t+1}$ (indicator)* | | | |
|---|---|---|---|---|
| | Model (1) | Model (2) | Model (3) | Model (4) |
| *CYBER_INSURANCE* | 0.457*** | 0.409*** | 0.413*** | 0.397*** |
| | (8.716) | (8.057) | (8.138) | (7.790) |
| *RISK_SECTION_LEGNTH* | -0.032*** | | | |
| | (-3.511) | | | |
| *HIGH_TECH* | | -0.651*** | | |
| | | (-5.901) | | |
| *TANGIBILITY* | | | 0.221 | |
| | | | (1.032) | |
| *ICW* | | | | -1.549*** |
| | | | | (-10.690) |
| Firm Characteristics Controls | Yes | Yes | Yes | Yes |
| Year Fixed Effects | Yes | Yes | Yes | Yes |
| Industry Fixed Effects | Yes | Yes | Yes | Yes |
| # Observations | 23257 | 23257 | 23257 | 23257 |
| Pseudo $R^2$ | 0.553 | 0.553 | 0.552 | 0.555 |
| Area under ROC | 0.950 | 0.950 | 0.950 | 0.955 |

Table 6 shows the association between firm disclosure of cyber insurance and probability of a future breach controlling for risk section length, High-Tech, tangibility, and internal control weaknesses. The sample consists of firm-year observations over the period 2010 to 2021. The dependent variable in each regression is probability of $BREACH_{t+1}$, an indicator variable that takes value of one if a firm experiences a breach in a year $t+1$ and zero otherwise. The independent variable of interest in Model (1) regression is *RISK_SECTION_LENGTH*, the natural log of file size of Item 1A. Risk Factors of 10-K filings for a firm *i* in year *t*; the independent variable in Model (2) is *HIGH_TECH*, an indicator variable equal to one if firm *i* belongs to one of these industries: drugs, R&D services, programming, computers, and electronics or zero otherwise; independent variable in Model (3) is *TANGIBILITY,* total property, plant, and equipment scaled by total assets for firm *i* in year *t*; and independent variable in Model (4) is *ICW*, an indicator variable equals one if firm $i$ reports internal control weaknesses in year $t$ and zero otherwise. The empirical model used in this table is Equation (1). The regression includes an intercept but is not tabulated for parsimony. All specifications include control variables, industry fixed effects, and year fixed effects. Appendix B contains details of these variables. The *t-statistics* are in parentheses and ***, **, and * indicate significance at the 0.01, 0.05, and 0.10 levels, respectively.

TABLE 7 Impact of Cyber Insurance on Breach Consequences Controlling for Industry Sector and CEO Power

| **Panel A:** Breach Consequences and Industry Sector | | | |
|---|---|---|---|
| *Dependent Variable* | *DISCLOSURE_ TIMELINESS* | *RESOLUTION_ TIMELINESS* | *BREACH_ FREQUENCY* |
| | Model (1) | Model (2) | Model (3) |
| *CYBER_INSURANCE* | 0.128*** | -0.381*** | 0.110*** |
| | (3.154) | (-3.929) | (4.831) |
| *BUSINESS_EQUIPMENT_AND_SOFTWARE* | -0.249 | 1.044** | 1.551*** |
| | (-1.137) | (2.112) | (12.672) |
| *WHOLESALE_AND_RETAIL* | -0.020 | -0.284 | 0.597*** |
| | (-0.088) | (-0.580) | (4.759) |
| *HEALTHCARE* | 0.145 | 1.070* | 0.998*** |
| | 0.610) | (1.920) | (7.655) |
| *FINANCE* | 0.168 | 0.518 | 1.156*** |
| | (0.800) | (1.105) | (9.851) |
| Firm and Breach Control Variables | Yes | Yes | Yes |
| Year Fixed Effects | Yes | Yes | Yes |
| Industry Fixed Effects | No | No | No |
| # Observations | 6239 | 1837 | 7411 |
| $R^2$ | 0.463 | 0.330 | 0.382 |
| **Panel B:** Breach Consequences and CEO Power | | | |
| *Dependent Variable* | *DISCLOSURE_ TIMELINESS* | *RESOLUTION_ TIMELINESS* | *BREACH_ FREQUENCY* |
| | Model (1) | Model (2) | Model (3) |
| *CYBER_INSURANCE* | 0.109*** | -0.334*** | 0.100*** |
| | (2.737) | (-3.586) | (4.476) |
| *CEO_POWER* | -0.040 | -0.091 | 0.062*** |
| | (-0.937) | (-0.883) | (2.588) |
| Firm and Breach Control Variables | Yes | Yes | Yes |
| Year Fixed Effects | Yes | Yes | Yes |
| Industry Fixed Effects | Yes | Yes | Yes |
| # Observations | 6622 | 1955 | 7835 |
| $R^2$ | 0.454 | 0.333 | 0.412 |

Table 7 estimates impact of cyber insurance on breach consequences controlling for whether breaches are more likely in certain industries (Panel A), and whether CEO power impacts the association between cyber insurance and breach consequences (Panel B). In Panel A, the regression includes five industry indicators defined using the Fama-French 12 industries and uses Manufacturing industry as a reference group. The dependent variable in Model (1) is *DISCLOSURE_TIMELINESS*, defined as natural long of time firm *i* takes to announce breach in year *t*; dependent variable in Model (2) is *RESOLUTION_TIMELINESS*, defined as natural log of time firm *i* takes to resolve the breach in year *t*; and dependent variable in Model (3) is *BREACH_FREQUENCY* defined as natural log of number of breach events for firm *i* in year *t*. In Panel (B), the regression includes *CEO_POWER*, defined as an indicator variable equal to one if the CEO for firm *i* is also the chair of the board in year *t*, and zero otherwise. The sample consists of firm-year observations over the period 2010 to 2021. The empirical model used in this table is Equation (3). The regression includes an intercept but is not tabulated for parsimony. All specifications include controls and year fixed effects. Appendix B contains details of these variables. The *t-statistics* are in parentheses and ***, **, and * indicate significance at the 0.01, 0.05, and 0.10 levels, respectively.

TABLE 8 Test of mean difference for propensity matched sample

| *Variables* | Firm-years with no cyber insurance (N= 6115): A | Firm-years with cyber insurance (N= 6115): B | Test of mean difference (A-B) |
|---|---|---|---|
| | Mean | Mean | Mean |
| *FIRM_SIZE* | 7.959 | 9.771 | -1.812*** |
| *FIRM_AGE* | 20.970 | 29.690 | -8.728*** |
| *ROA* | 0.042 | 0.047 | -0.005 |
| *LEVERAGE* | 0.276 | 0.262 | 0.014*** |
| *LOSS* | 0.160 | 0.130 | 0.035*** |
| *R&D_EXPENDITURE* | 0.016 | 0.017 | -0.001 |
| *CASH_HOLDINGS* | 0.089 | 0.088 | 0.001* |
| *CIO_ROLE* | 0.120 | 0.220 | -0.092*** |
| *CYBER_RISK* | 0.680 | 0.830 | -0.151*** |
| *PAST_BREACH* | 0.020 | 0.040 | -0.024*** |
| *COMPLIANCE_COMMITTEE* | 0.040 | 0.060 | -0.017*** |
| *RISK_COMMITTEE* | 0.120 | 0.180 | -0.055*** |
| *TECHNOLOGY_COMMITTEE* | 0.040 | 0.060 | -0.025*** |
| *COMPLEXITY* | 1.845 | 2.129 | -0.285*** |
| *HIGH_TECH* | 0.090 | 0.090 | -0.001 |
| *PEER_CYBER_INSURANCE* | 0.000 | 0.501 | -0.501*** |
| *PEER_NUM* | 4.200 | 4.361 | -0.161*** |

Table 8 shows the means for a sample of 6,115 firm-year observations that disclose cyber insurance and a propensity-matched sample of 6115 firm-year observations that do not disclose cyber insurance over the period 2010 to 2021. Appendix B provides detailed descriptions of the construction of the variables. ∗∗∗, ∗∗, and ∗ denote that *t-tests* for mean differences are significant at the 1%, 5%, and 10% levels, respectively.

TABLE 9 Endogeneity and Sample Selection Bias

| | **PSM** | **2SLS** | | **Heckman** | |
|---|---|---|---|---|---|
| | | First Stage | Second Stage | First Stage | Second Stage |
| | Model 1 | Model 2 | Model 3 | Model 4 | Model 5 |
| *CYBER_INSURANCE* | 2.728*** | | 0.738*** | | 2.642*** |
| | (27.385) | | (11.566) | | (15.593) |
| *PEER_CYBER_INSURANCE* | | 7.691*** | | | |
| | | (68.487) | | | |
| *PEER_NUM* | | 0.138*** | | | |
| | | (10.368) | | | |
| *L_PEER_CYBER_INSURANCE* | | | | 9.357*** | |
| | | | | (75.095) | |
| *L_PEER_NUM* | | | | 0.126*** | |
| | | | | (9.130) | |
| *IMR* | | | | | 5.510*** |
| | | | | | (13.783) |
| Controls | Yes | Yes | Yes | Yes | Yes |
| Year Fixed Effects | Yes | Yes | Yes | Yes | Yes |
| Industry Fixed Effects | Yes | Yes | Yes | Yes | Yes |
| Observations | 12230 | 23257 | 23257 | 23257 | 23257 |
| Area under ROC | 0.460 | 0.523 | 0.554 | 0.539 | 0.556 |
| Pseudo $R^2$ | 0.946 | 0.956 | 0.951 | 0.962 | 0.952 |

Table 9 presents several tests to control for endogeneity and sample selection bias. Model (1) reports the propensity-matched regression results of *CYBER_INSURANCE* and the probability of a future $BREACH_{t+1}$. Each cyber insurance firm-year is matched with one control firm-year based on firm size, age, profitability, industry sector (Fama-French 12), and fiscal year. Models (2) and (3) present the 2SLS regression results. Model (2) reports the first-stage regression results, where *CYBER_INSURANCE* is the dependent variable and *PEER_CYBER_INSURANCE* and *PEER_NUM* are the instruments. The empirical model used in this model is Equation (2). Model (3) shows the second-stage regression results of *CYBER_INSURANCE* and the probability of a $BREACH_{t+1}$. Models (4) and (5) show Heckman's (1979) two-stage regression results. Model (4) shows the first-stage regression results for the firm's choice to purchase cyber insurance (Equation 2), where *L_PEER_CYBER_INSURANCE* and *L_PEER_NUM* are used as instruments. Model (5) shows the second-stage regression results of *CYBER_INSURANCE* and probability of a future $BREACH_{t+1}$, controlling for the inverse Mills ratio (*IMR*). All variables are defined in detail in Appendix B. For parsimony, only variables of interest are reported. The regression includes an intercept but is not tabulated for parsimony. The *t-statistics* are in parentheses and *, **, and *** indicate significance at the 10%, 5% and 1% levels, respectively.

**Appendix A: Item IA Risk Factors section snippets around cyber insurance**

**Apple Inc. | 2018 Form 10-K | page 15**
To help protect customers and the Company, the Company deploys and makes available technologies like multifactor authentication, monitors its services and systems for unusual activity and may freeze accounts under suspicious circumstances, which, among other things, can result in the delay or loss of customer orders or impede customer access to the Company's products and services. While the Company maintains insurance coverage that is intended to address certain aspects of data security risks, such insurance coverage may be insufficient to cover all losses or all types of claims that may arise.

**Morgan Stanley | 2019 Form 10-K | page 14**
While many of our agreements with partners and third-party vendors include indemnification provisions, we may not be able to recover sufficiently, or at all, under such provisions to adequately offset any losses we may incur. In addition, although we maintain insurance coverage that may, subject to policy terms and conditions, cover certain aspects of cyber and information security risks, such insurance coverage may be insufficient to cover all losses.

**Johnson & Johnson | 2018 Form 10-K | page 9**
This impact could result in reputational, competitive, operational or other business harm as well as financial costs and regulatory action. The Company maintains cybersecurity insurance in the event of an information security or cyber incident; however, the coverage may not be sufficient to cover all financial losses.

**T-Mobile | 2017 Form 10-K | page 12**
If we or our third-party suppliers are subject to such attacks or security breaches, we may incur significant costs or other material financial impacts, which may not be covered by, or may exceed the coverage limits of, our cyber insurance, be subject to regulatory investigations, sanctions and private litigation, experience disruptions to our operations or suffer damage to our reputation.

**Merck & Co., Inc. | 2017 Form 10-K | page 24**
Merck does not expect a significant impairment to the value of intangible assets related to marketed products or inventories as a result of the cyber-attack. The Company has insurance coverage insuring against costs resulting from cyberattacks and has received proceeds. However, there may be disputes with the insurers about the availability of the insurance coverage for claims related to this incident.

## Appendix B: Variable definitions

This table provides detailed descriptions of all the variables used in the tables. All names within square brackets refer to Compustat item names.

| Variable | Description | Source |
|---|---|---|
| *ACTORS* | Indicator variable for whether a cyber-attack is initiated by internal or external actors. | Advisen |
| *BREACH* | An indicator variable equals to one if the firm *i* has reported a breach in the year *t*, or zero otherwise. | Advisen |
| *BREACH_FREQUENCY* | Natural log of number of breach events for firm $i$ in year $t$. | Advisen |
| *BREACH_TYPE* | Based on Advisen classification of cyberattacks coded as Data, Privacy, and Other as follows: (1) Data: malicious breach; physically lost or stolen; and unintentional disclosure. (2) Privacy: unauthorized contact or disclosure and unauthorized data collection. (3) Other: industrial controls & operations; IT- configuration/ implementation errors and processing errors; network/website disruption; skimming, physical tampering; identity - fraudulent use/account access; and phishing, spoofing, social engineering. | Advisen |
| *CASH_HOLDINGS* | The ratio of cash and short-term investments [che] scaled by total assets [at] for firm *i* in year *t*. | Compustat |
| *CEO_POWER* | An indicator variable equals one if the CEO for firm *i* is also the chair of the board in year *t,* and zero otherwise. | BoardEx |
| *CIO_ROLE* | An indicator variable equals one if firm *i*'s top management team has a CIO, Chief Information Security Officer, Chief Security Officer, or Chief Technology Officer in year *t,* or zero otherwise. | BoardEx |
| *COMPLEXITY* | Number of business (BUSSEG) and geographic (GEOSEG) segments for firm *i* in year *t.* | Compustat |
| *COMPLIANCE_COMMITTEE* | An indicator variable equals to one if firm *i* discloses the presence of a "compliance committee" at the board-level in year *t* prior to the date of the breach, or zero otherwise. | BoardEx |
| *CYBER_INSURANCE* | An indicator variable equals to one if firm *i* discloses cyber insurance in "Item 1A. Risk Factors" of 10-K filings in year *t,* or zero otherwise. | 10-K |
| *CYBER_RISK* | An indicator variable equals to one if firm *i* belongs to one of the following industries: financial services, healthcare, retail, manufacturing, or information and communications in year *t*, or zero otherwise (NAICS 31, 32, 33, 44, 45, 51, 52, and 62). | Compustat |
| *DISCLOSURE_TIMELINESS* | Natural log of number of days between the discovery date and the first notice date of a breach for firm $i$ in year $t$. | Advisen |
| *FIRM_AGE* | The age of firm *i* in years as of year *t.* Fiscal year – the year that the firm first appeared in Compustat. | Compustat |
| *FIRM_SIZE* | Natural log of firm *i*'s total assets in year *t.* | Compustat |
| *HIGH_TECH* | An indicator variable equal to one if firm *i* belongs to one of these industries: drugs (SIC codes 2833–2836), R&D services (8731–8734), programming (7371–7379), computers (3570–3577), and electronics (3600–3674); or zero otherwise. | Compustat |
| *ICW* | Indicator variable equal one if firm $i$ reports internal control weaknesses in year $t$ and zero otherwise. | Audit Analytics |
| *IMR* | The inverse Mills ratio from the estimation of Equation (2). | |
| *INFORMATION_TYPE* | Type of data, information, or assets compromised coded as *Corporate* including Corporate Loss of Business | Advisen |

| Variable | Description | Source |
|---|---|---|
| | Income/Services, Corporate Loss of Digital Assets, and Corporate Loss of Financial Assets, and *Personal* covering: Personal Financial Identity, Personal Health Information, and Personal Identity Information. | |
| *LEVERAGE* | Long-term debt [dltt] plus debt in current liabilities [dlc], scaled by total assets [at] for firm *i* in year *t*. | Compustat |
| *LOSS* | Indicator variable equal to one if firm *i* exhibits operating income before depreciation [oibdp] less than zero in year *t,* or zero otherwise. | Compustat |
| *L_PEER_CYBER_INSURANCE* | Percentage of firms within the same state as firm *i* that disclose cyber insurance in year *t*. | |
| *L_PEER_NUM* | Natural log of the number of firms within the same state as firm *i* that disclose cyber insurance in year *t*. | |
| *PAST_BREACH* | Indicator variable equal to one if the firm *i* had a reported breach on Advisen in the fiscal year $_{t-1}$ or zero otherwise. | Advisen |
| *PEER_CYBER_INSURANCE* | Percentage of firms within the same industry (Fama-French 12) as firm *i* that disclose cyber insurance in year *t*. | |
| *PEER_NUM* | Natural log of the number of firms within the same industry (Fama-French 12) as firm *i* in year *t*. | |
| *R&D_EXPENDITURE* | Natural log of firm *i*'s research and development expenditures [xrd] to total assets [at] in year *t.* Missing values are replaced with zero. | Compustat |
| *RESOLUTION_TIMELINESS* | Natural log of number of days between the original loss start date and original loss end date of a breach for firm *i* in year *t*. | Advisen |
| *RISK_SECTION_LENGTH* | Natural Log of file size of Item 1A. Risk Factors of 10-K filings for a firm *i* in year *t*. | 10-K |
| *RISK_COMMITTEE* | An indicator variable equal to one if firm *i* discloses the presence of a "risk committee" at the board-level in year prior to the date *t* of the breach, or zero otherwise. | BoardEx |
| *ROA* | Operating income before depreciation [oibdp] scaled by total assets [at] for firm *i* in year *t.* | Compustat |
| *SEVERITY* | Natural log of number of identities breached or stolen, social security numbers revealed, devices compromised, etc. | Advisen |
| *SOURCE* | Source of data, assets, or information that has been compromised, or resulted in the cyber incident involves laptop, point of sales, among others. Coded as: (1) Client Hardware; (2) Server, Cloud, and Web; (3) Telecommunication; (4) Privacy Law Violations; and (5) Others. | Advisen |
| *TANGIBILITY* | Total property, plant, and equipment [ppent] scaled by total assets [at] for firm *i* in year *t.* | Compustat |
| *TECHNOLOGY_COMMITTEE* | An indicator variable equal to one if the firm *i*'s discloses the presence of a "technology committee" at the board-level in year *t* prior to the date of the breach, or zero otherwise. | BoardEx |

## Chapter 5: Conclusion

Cybersecurity risk represents an omnipresent concern and threat to firms as it is a major global problem with an evolving and dynamic nature, and with the highest likelihood of occurrence in the coming years. With cyber incidents increasing in frequency, severity, and impact, and the growing pressure from investors, media, regulators, and other stakeholders, effective cybersecurity risk governance and management have become more pressing than ever before. This dissertation comprises three essays that contribute to the discussion on research related to cybersecurity risk and incident disclosure, as well as the governance and management of cybersecurity risks and incidents.

The first essay provides an overview of the current state of cybersecurity risks and incidents disclosure as covered in the extant literature. Based on the synthesis of previous studies' results, the essay finds that various factors, including regulatory and institutional pressure, public pressure, board governance and firm characteristics, peer effects, and the characteristics of a cyber incident, motivate companies to disclose information related to cybersecurity risks and incidents. Moreover, the synthesis reveals that, while the informativeness of cybersecurity risks and incidents disclosures aligns with the expectations of regulators in terms of usefulness to equity markets, their quality falls short.

The second essay examines the governance of cybersecurity through the lens of the board of directors' cybersecurity risk oversight responsibility assignment. The analysis reveals a wide variation in cybersecurity risk oversight responsibility assignment but most firms across industry sectors delegate it to the audit committee. Moreover, the results suggest that board's cyber experience and network size are significant factors of explicit assignment of oversight responsibility, smaller boards increase the likelihood that the full board will oversee cybersecurity

risk as opposed to a board-level committee, and while boards with more equity ownership and cybersecurity experience tend to delegate oversight to the audit committee, bigger boards with higher network size are more likely to assign it to a non-audit committee. Furthermore, the results confirm that the audit committee is the default option for assigning oversight responsibility. In the event of a breach, the presence of oversight decreases the time firms take to announce and resolve such a breach as well as the recurrence of breaches. Moreover, the results indicate that while audit committee oversight is more effective in timeliness of breach disclosure and resolution, full board oversight is more effective in reducing breach recurrence.

Focusing on cybersecurity risk management, the third essay investigates whether firms that disclose their cyber insurance are more susceptible to data breaches and how effective cyber insurance is in the event of a breach. The essay finds that companies that disclose their cyber insurance are more likely to experience a future data breach and that having cyber insurance contributes to delayed public breach disclosure, more timely breach resolution, and higher breach recurrence.

The essays contained in this dissertation make valuable contributions to the literature on disclosure, risk governance, and cybersecurity. Specifically, the first essay provides a comprehensive overview and insights on various components of cybersecurity risks and incidents disclosure, including its determinants, informativeness, content, and quality. It also expands the existing literature on narrative disclosures and content analysis by highlighting the state of narrative sections in corporate filings. The second essay complements and expands an emerging stream of cybersecurity governance literature by examining who is responsible for cybersecurity risk oversight. It also focuses on both the governance determinants of oversight assignment and the impact of such assignment on the economic consequences of a cyber breach event, identifying

governance determinants that are relevant to the oversight assignment and those that are more related to the way oversight is distributed between the full board and board-level committee. The third essay contributes to the cybersecurity literature by examining both pre- and post-impacts of a cybersecurity risk management strategy, specifically risk transfer via cyber insurance. Additionally, it provides managers with an additional factor to consider when determining their disclosure policy by suggesting that revealing the presence of cyber insurance may serve as an incentive for potential cyber-attacks. Overall, the three essays make valuable contributions to the literature on cybersecurity risks and incidents disclosure, governance, and management.

The essays contained in this dissertation also provide practical implications. Specifically, the first essay highlights cybersecurity risk and incident reporting practices, as well as preventive and mitigation measures used to address them, and provides insights to practitioners on factors motivating firms to disclose cybersecurity risks. This information can enable practitioners to devise strategies that enhance cybersecurity reporting without increasing vulnerability. Moreover, to optimize cybersecurity disclosure, firms need to develop a disclosure policy that balances standardization and firm specificity, complies with local and international regulations, and accommodates various stakeholders. The findings of the second essay offer timely and relevant evidence to understand cybersecurity oversight leading practices, highlighting the managerial implications of setting the right "tone at the top" for oversight responsibility and carefully choosing the oversight governance structure that best fits the board's characteristics. Finally, the findings of the third essay inform practitioners, regulators, and policymakers as they evaluate their cybersecurity risks policies and the effectiveness of their cybersecurity risks countermeasures, especially given that cyber insurance disclosure is still voluntary.

The findings of the last two essays also provide insights to the regulator. Particularly, the findings of the second essay confirm the effectiveness of board explicit cybersecurity risk oversight in the event of a breach provides valuable input to the regulator, which has prioritized cybersecurity risk governance and disclosure as evidenced by the SEC's proposed rule to require disclosure about the board's oversight of cybersecurity risk. Furthermore, the third essay findings offer valuable input to regulators and policymakers seeking to develop more effective cybersecurity regulations, such as the proposed California State Assembly-Bill 2320, which would mandate businesses that retain customer data to maintain cyber insurance coverage.

The studies in this dissertation are subject to some limitations, addressing them could be fruitful for future research. A potential limitation is that although the search strategy uses the terminology commonly used by the SEC, it may not have captured all relevant proxy statements. It is also possible that other determinants may provide additional insights into the relation between oversight assignment and breach consequences. Moreover, the essays adopt an association-based approach, and as such, the capacity to establish causal links is limited. A further limitation is that due to limited availability of data, the essays do not consider the actual economic cost of a breach.