ESSAYS ON THE RISE OF DIGITAL UPPER ECHELONS: IMPLICATIONS TO FIRM INNOVATION, CYBERSECURITY, AND GOVERNANCE

A Dissertation
Submitted to
the Temple University Graduate Board

In Partial Fulfillment
of the Requirements for the Degree
DOCTOR OF PHILOSOPHY

by
Yiwen Gao
August 2023

Examining Committee Members:

Sunil Wattal, Advisory Co-Chair, Department of Management Information Systems
Jason Thatcher, Advisory Co-Chair, Department of Management Information Systems
Solon Moreira, Department of Management
John D'Arcy, University of Delaware
Oleg Rytchkov, External Reader, Department of Finance

ABSTRACT

The rapid development of technology and the associated new challenges such as cybersecurity risk triggered the rise of new digital upper echelons such as Chief Digital Officers (CDOs) or Chief Information Security Officers (CISOs). However, there is a lack of theoretical understanding and rigorous empirical examination regarding the impacts of emerging digital upper echelon roles on firm performance. This dissertation develops three essays that examine the rising digital upper echelons' implications for firm innovation, cybersecurity strategies, and governance.

The first essay examines the antecedents of CISO presence on the TMT and its consequences for firm innovation. We conduct a longitudinal empirical analysis using a unique dataset of S&P 1500 firms from several secondary sources. Our study shows that a firm's appointment of a CISO in TMT is positively influenced by the CISO presence in TMT of industry peers and their data breaches. Importantly, we find that CISO presence in TMT increases firms' innovation on average. The presence of a CISO in TMT with more experience in the same industry as the focal firm has a stronger effect on innovation, while CISOs in TMT with more experience in other industries only increase innovation when the firm's industry is not very turbulent. We also found that CISOs in TMT with a business or IT education have a stronger positive impact on firm innovation. This research is the first to assess the impact of CISO presence in TMT on non-security outcomes. We shed new light on the drivers of why firms appoint a CISO to TMT and how CISO presence in TMT impacts firm value beyond the security function. Our findings also provide managers with a nuanced understanding of how CISO backgrounds

impact innovation and provide guidance for hiring CISOs who align with the firm's information management and innovation goals.

The second essay focuses on how competing incentive systems (e.g., compensation) shape digital upper echelons and non-digital upper echelons impact on the firm's disclosure of data breaches in SEC fillings and the moderating role of board members' cybersecurity intensity on upper echelon members' disclosure. We draw on the agency theory to develop a theoretical model considering the divergent priorities and goals of the digital and non-digital upper echelons involved. We conducted a longitudinal analysis of public firms that have experienced data breaches. Results demonstrate that increased digital upper echelons' compensation will lead to timelier SEC data breach notifications, whereas increased non-digital upper echelons' compensation will have the opposite effect. Board cybersecurity intensity weakens the positive impacts of digital upper echelons' compensation but amplifies the negative impacts of non-digital upper echelons' compensation on notification timeliness. Hence, our findings counter the view that cybersecurity experience on the board speeds up reporting of data breaches by upper echelons. This study also delineates the differences on incentive systems between digital and non-digital upper echelons in SEC data breach notifications. Our results provide managerial implications on how to incentivize firms to disclose data breaches in SEC in a timely manner.

The third essay compares two different reporting structures of CDOs and CISOs: within-group reporting structure (i.e., report to IT heads) versus across-group reporting structure (i.e., report to non-IT heads). Since reporting structure needs to be aligned with firm strategic visions, we examine (1) how CDOs' reporting structure and digital transformation jointly affect firm performance, and (2) how CISOs' reporting structure and security awareness jointly affect firm performance. We conducted a longitudinal analysis using a unique dataset collected from multiple sources. Our results demonstrate that compared with within-group reporting structure, CDOs reporting to non-IT heads weakens the positive relationship between digital transformation and the firm's prospective performance (i.e., market-to-book ratio of assets). However, CISOs reporting to non-IT heads weakens the negative relationship between security awareness and the firm's retrospective performance (i.e., operational incomes). Overall, our results highlight the advantages of CDOs' within-group reporting structure and CISOs' across-group reporting structure. This research contributes to our understanding of how CDOs' and CISOs' reporting structure aligns with firm strategic visions in shaping firm performance. Our findings offer implications to business managers on designing reporting structures and governing emerging IT executives.

Overall, this three-essay dissertation enriches our understanding of the impacts of rising digital upper echelons and effective ways to govern these emerging top management roles.

ACKNOWLEDGMENTS

The culmination of this dissertation signifies the conclusion of my extensive PhD expedition, an accomplishment that would not have been feasible without the unwavering support and encouragement from numerous individuals.

I would like to sincerely convey my gratitude to my committee co-chairs Dr. Sunil Wattal and Dr. Jason Thatcher for their invaluable guidance throughout the journey. Their insightful input has shaped my research mindset. They have also kindly offered me unconditional support throughout my journey in the program. My appreciation goes to Dr. John D’Arcy for his willingness to provide tremendous help as a coauthor as well as to serve on my committee. I also indebtedly thank Dr. Solon Moreira and Dr. Oleg Rytchkov for providing insightful suggestions to improve the paper to be better prepared with journal submission.

I would also like to take a moment to thank for all faculty who has touched my life in various way – teaching, working with, helping, and supporting me – Dr. Min-Seok Pang, Dr. Sezgin Ayabakan, Dr. Munir Mandviwalla, Dr. Detmar Straub, Dr. Aleksi Aaltonen, Dr. JaeHwuen Jung, Dr. David Schuff, Dr. Konstantin Bauman, Dr. Anthony Vance, and Dr. Taha Havakhor.

Thanks for all research and life suggestions coming from Aaron Cheng, Ada Wang, Alvin Zheng, Xue Guo, Siddharth Bhattacharya, Zhe Deng, Xi Wu and Leting Zhang. Special thanks to my cohorts, Youngjin Kwon and Hyeonsik Shin, for supporting each other to survive. I also appreciate all the thoughtful and interesting discussion with Jack Shan, Mohammod Rahman, Dongwook Chun, Meixian Wang, Kanghyun Cho, Ziyi Zhao, Yutong Zhang, and Shuhua Wu. In addition, thanks to my friends who have provided me with all the suggestions and support during this journey - Yueru Qin, Dishi Hu, Yuqian Chang, Wenchu Li, and Yaming Gong.

Last but not least, my heartfelt gratitude goes to all my family members. Thanks to my parents, aunts, and uncles for raising me up with love. Thanks to all my cousins for taking pressure away from their little sister and supporting me in numerous ways, which enables me the freedom to do whatever I would like. I am proud of being born in this family and sincerely appreciate their unconditional love.

TABLE OF CONTENTS

ABSTRACT iii

ACKNOWLEDGMENTS vi

LIST OF TABLES xiv

LIST OF FIGURES xv

CHAPTER

1. INTRODUCTION 1

2. CHIEF INFORMATION SECURITY OFFICERS IN TOP MANAGEMENT TEAMS: IMPACT ON FIRM INNOVATION 8

    Introduction 8

    Literature Review 12

        Digital Upper Echelons and Firm Innovation 12

        Antecedents of Upper Echelon Presence in TMT 14

    Hypothesis Development 15

        Antecedents of CISO Presence in TMT 15

        CISO Presence in TMT and Firm Innovation 17

        Impact of CISO Industry Experience 21

        Impact of Industry Turbulence 24

    Method 27

        Data 27

        Variable Definitions 28

        Empirical Approach 32

    Results 33

Results of Hypothesis Testing 35

Addressing Endogeneity Concerns 38

Mechanisms 39

Falsification Tests 41

Post-Hoc Analyses: Impacts of CISO Educational Backgrounds.............43

Additional Robustness Checks Using Alternative Measures.....................44

Discussion 45

Summary of Main Findings 45

Theoretical Implications 47

Practical Implications..50

Limitations and Future Research 52

Conclusion 53

3. THE INFLUENCES OF EXECUTIVE COMPENSATION AND BOARD CYBERSECURITY INTENSITY ON SEC DATA BREACH NOTIFICATION TIMELINESS 54

Introduction 54

Background on the SEC Data Breach Notification Decision 57

Theoretical Foundation 59

Executive Compensation and Decision-Making for IT and Non-IT Executives 59

Hypothesis Development 61

Executive Compensation and SEC Data Breach Notification Timeliness..61

Moderating Influence of Board of Directors' Cybersecurity Intensity 64

Method 67

Data 67
Variable Definitions 68
Empirical Approach 71
Results 74
Results of Hypothesis Testing 74
Addressing Endogeneity Concerns 76
Mechanisms and Additional Robustness Checks 79
Discussion 89
Theoretical Contributions 92
Practical Implications 94
Future Research Directions 96
Limitations 97
Conclusion 98
4. TO WHOM SHOULD CDOS AND CISOS REPORT? MODERATING IMPACTS ON DIGITAL TRANSFORMATION AND SECURITY AWARENESS 99
Introduction 99
Literature Review 102
The Rise of Digital Upper Echelons 102
Reporting Structure of Digital Upper Echelons 103
Social Categorization Processing 106
Hypothesis Development 107
Effects of Digital Transformation on Firm Performance 109
Effects of Security Awareness on Firm Performance 111
Moderating Effects of CDO Reporting Structure 113

Moderating Effects of CISO Reporting Structure 115

Method 116

Data 116

Variable Definitions 117

Empirical Approach 122

Results 124

Results of Hypothesis Testing 124

Robustness Checks 127

Discussion 134

Theoretical Implications 135

Practical Implications 136

Limitations and Future Research 137

5. DISCUSSIONS AND CONCLUSION 138

REFERENCES 143

APPENDICES

A. Correlation Table of CISO Presence Paper...159

B. Results of Two-Stage Least Square Model 160

C. Measurement of Risk-Seeking Incentive – Vega 161

D. Results of Falsification Tests 164

E. Coding of CISO Educational Background 166

F. Results of Additional Robustness Checks 169

G. Cybersecurity-Related 8-K Keywords for SEC Data Breach 171

H. Coding of IT Executive Positions and Examples..172

I. Correlation Table of Compensation and Data Breach Disclosure Paper..........173

J. Correlation Table of Reporting Structure Paper...175

LIST OF TABLES

Table Page

1. Descriptive Statistics of CISO Presence in TMT Paper 31
2. Summary of Empirical Analyses 34
3. Results of CISO Presence Hypothesis Testing 36
4. Descriptive Statistics of Compensation and Data Breach Disclosure Paper 72
5. Survival Analysis of Main and Moderating Effects.. 75
6. Control Functions.. 78
7. Results Using Compensation Incentive Ratio 80
8. Survival Analysis of Moderating Effects with Alternative Compensation 82
9. Survival Analysis of Main and Moderating Effects using
   Quarter Fixed Effect 86
10. CEO and Non-CEO Compensation Impacts on Disclosure................................ 88
11. CEO, CFO, and Others' Compensation Impacts on Disclosure 90
12. Descriptive Statistics of Reporting Structure Paper.. 121
13. Results of IT Strategy and Reporting Structure Hypothesis Testing 125
14. Industry-Specific Linear Time Trend Model 127
15. Alternative Definition for IT Industry 129
16. Falsification Test - Impacts in IT Industry... 132

LIST OF FIGURES

Figure Page

1. The Research Model of CISO Presence in TMT 26

2. Reporting Structure Definition 108

3. The Research Model of Reporting Structure 109

CHAPTER 1

INTRODUCTION

Organizations are constantly facing the opportunities and challenges brought by rapid changes in Information Technology (IT). The upper echelon perspective suggests that top management team (TMT) members influence firm decisions and shape outcomes (Hambrick & Mason, 1984). As technology continues to evolve at an unprecedented rate, the role of IT leadership becomes increasingly vital in shaping the strategic direction and ensuring the success of organizations across sectors.

The emergence of IT adoption and implementation in firms increase the demands of Chief Information Officer (CIO) in the last century, which marks the inception of IT leadership literature in academic research. In the first wave of IT usage in firms, IT function was mostly treated as the supporting of business operations (Neumann & Zviran, 1997). Accordingly, the primary responsibility of CIOs lies in safeguarding and proactively equipping firms to confront the technology revolution (Maruca, 2000). At the beginning of the 21st century, IT starts to move beyond just supporting the business to play a role in generating and sustaining business value for firms by developing the next new technologies (Blackburn et al., 1998) and realizing business goals (Prattipati & Mensah, 1997). Meanwhile, the preferred CIO capabilities shift from a singular technical focus to a wide spectrum of technology, leadership, business systems thinking, and relationship building, etc. (Feeny & Willcocks, 1998). With this transformation, CIOs' role evolves from a technical position to a more strategic position within the firm.

With the changing focus of the CIO role, research about CIOs has tackled major themes: (a) CIOs' relationship with CEO, (2) CIOs' relationship with other top management team (TMT) members, and (3) CIOs' impacts in the firm. First, the CIO's previous technical focus mindset gives them a difficult time communicating with CEO and other TMT members, who have limited knowledge about technical issues. Previous literature argues that if the CEO and CIO have a closer arrangement, the impacts of IT investments on firm performance will be amplified (Li & Ye, 1999). Whether the CEO and CIO have mutual understanding or similar perceptions in terms of IT vision depends on such factors as national culture, industry (Tai & Phelps, 2000), communication frequency and channel richness (Johnson & Lederer, 2005). This mutual understanding will in turn improve the alignment of IT and business strategy (Johnson & Lederer., 2010). Beyond mutual understanding, the alignment of CIO reporting structure and firm strategy can be beneficial for firm performance (Banker et al., 2011).

Second, in terms of the relationship between CIO and other TMT members, CIO first needs to get commitment from their peers, e.g., Chief Financial Officer (CFO) and Chief Operations Officer (COO), so that they can execute strategic information systems projects (Enns et al., 2001). Similar as the relationship with CEO, the mutual understanding between CIO and other TMT members can help improve the IS strategic alignment (Preston & Karahanna, 2009). In addition, the different dimensions of social capital in CIO-TMT relationship can influence firms' business value creation (Karahanna & Preston, 2013). In terms of their similarity and influence on their peers, CIO and other TMT members have similar survivability of job tenure (Dawson et al., 2015). CIO with the technical background can influence other TMT members and success in projects (Enns et al., 2001).

Third, the designation of CIO position can be beneficial for the firms as well. In the industries that are undergoing IT driven transformation, the announcement of a new CIO position can boost firm performance (Chatterjee et al., 2001); and this impact applies compared with designation of marketing managers (Taylor & Vithayathil, 2018). Research has also demonstrated that appointing a CIO to the board of directors increases the firm's market value and long-term performance (Bandodkar & Grover, 2022).

CIO characteristics, such as their attitude towards IT investments (Sobol & Klein, 2009), human capital, structural power (Chen et al., 2010), strategic leadership (Leidner et al., 2010), and their relationships with authorities (Dawson et al., 2016) significantly influence firm performance measures, such as IT innovation, IT's contribution to firm efficiency, IT's contribution to strategic growth. In addition, the CIO's business and technical background have been discussed frequently. For CIO with decisional and interpersonal roles, the technical background will become critical (Carter et al., 2011). This technical background is highly related with where they are hired from and who or how they spend time once they are hired (Jones et al., 2020).

With the increasing demand for digital transformation and the complexity of digitalization, firms are appointing new technology-related executive positions (i.e., digital upper echelons) whose responsibilities go beyond the established CIO role (Tumbas et al., 2018), such as chief digital officer (CDO), chief information security officer (CISO), chief privacy officer, chief data officer, etc. Among them, from 2015 to 2018, 19% of top firms hired CDOs (LeadershipNetwork, 2018) and 60% of European organizations and 52.8% of US organizations have a CISO or equivalent position (Kappelman et al., 2019). These emerging digital upper echelons are inherently different from CIOs. For example, CIO is specialized in strategic IT, while emerging digital upper echelons have focused responsibilities in other aspects, such as digital transformation specialist and data specialist (Singh and Hess, 2017). Despite the prevalence of emerging digital upper echelons and their inherent differences from CIOs, research studying these emerging leaders, especially their impacts on business operations and value creation, is scant. The limited literature has focused on conceptualizing an emerging digital upper echelon role and describing the role's responsibilities. For example, the CDO is responsible for navigating digitalization (Tumbas et al., 2018), and CISO mainly focuses on how to mitigate cybersecurity concerns (Kappelman et al., 2020). Several studies have examined CDO's influence, such as their contingent impact on digital transformation signaling impact (Metzler et al., 2021).

Therefore, this dissertation develops three essays to understand the rising digital upper echelons' implications for firm innovation, cybersecurity strategies, and governance. The first essay examines how the appointment of CISO to TMT influences firm innovation and its boundary conditions. A longitudinal analysis of S&P 1500 firms demonstrates that firms with CISO presence in TMT, on average, have greater innovation outcomes than those without a CISO in TMT. Importantly, CISOs with richer experience in the focal firm's same industry have a greater impact on innovation. CISOs with richer experience in other industries boost innovation only when the firm's industry is less turbulent. We also found that CISOs with business or IT educational backgrounds have a stronger positive impact on firm innovation. This essay sheds new light on how CISOs in

TMT impact innovation beyond security. Our findings also offer nuances to our understanding of how various CISO backgrounds impact firm innovation, providing managerial implications for aligning the selection of CISOs in TMT with firm goals.

The second essay focuses on how incentives of digital upper echelons and non-digital upper echelons influence the firm's timely disclosure of data breaches and the moderating role of board members' cybersecurity intensity through interlocked firms' data breach experience. We draw on the agency theory to develop a theoretical model considering the divergent priorities and goals of the digital and non-digital upper echelons involved. We conducted a longitudinal analysis of public firms that have experienced data breaches. Results demonstrate that increased digital upper echelons' compensation will lead to timelier SEC data breach notifications, whereas increased non-digital upper echelons' compensation will have the opposite effect. Board cybersecurity intensity weakens the positive impacts of digital upper echelons' compensation but amplifies the negative impacts of non-digital upper echelons' compensation on notification timeliness. Hence, our findings counter the view that cybersecurity experience on the board benefits the firm and its stakeholders (e.g., improved cybersecurity decision-making and efficient information flow).

The third essay compares the impacts of two reporting structures for CDOs and CISOs, i.e., within-group reporting structure (i.e., report to IT heads) versus across-group reporting structure (i.e., reporting to non-IT heads). Prior reporting structure literature emphasized on firms' reporting structure in align with their strategic visions (Banker et al., 2011; Lee et al., 2015). CDOs are often responsible for digital transformation initiatives. We thus examine how firms' digital transformation and CDO reporting structure jointly influence firm performance. Given that CISOs' primary responsibilities reside in firm security management, we investigate how firms' security awareness at the firm-level and CISO reporting structure jointly affect firm performance. We focus on both retrospective (i.e., short-term, operational performance, such as operating incomes) and prospective (i.e., long-term, growth opportunities, such as market-to-book ratio of assets) performance for firms because IT has shown to create value at multiple levels, such as business processes, firm, and market (Kohli et al., 2012). Our longitudinal empirical analysis of S&P 1500 firms demonstrates that compared to within-group reporting structure, CDOs' across-group reporting structure weakens the positive relationship between digital transformation and the firm's prospective performance. However, CISOs' across-group reporting structure weakens the negative relationship between security awareness and the firm's retrospective performance, compared to CISOs' within-group reporting structure. Overall, our findings demonstrate the advantages of CDOs' across-group reporting structure (i.e., reporting to IT heads) and CISOs' across-group reporting structure (i.e., reporting to non-IT heads). This research contributes to our understanding of how CDOs' and CISOs' reporting structure influence firm performance in conjecture with firm strategic visions tied to their primary responsibilities. Our findings offer implications to business managers on designing reporting structures and governing CDOs and CISOs.

Overall, this dissertation is expected to enrich our understanding of the governance and impacts of the rising digital upper echelons. The three essays, collectively, suggests the importance of appointing emerging digital upper echelons to the TMT (e.g., CISO presence in TMT), governing them through reporting structures (e.g., CDOs’ and CISOs’ reporting structure), and the compensation of digital upper echelon group as compared with the non-digital upper echelon group’s compensation. This dissertation also covers a wide spectrum of impacts that the rising IT executive roles have, such as boosting firm innovation, speeding up the strategic disclosure of cybersecurity breaches, and amplifying the returns from emerging strategic visions such as digital transformation and security awareness.

CHAPTER 2

CHIEF INFORMATION SECURITY OFFICERS IN TOP MANAGEMENT TEAMS: IMPACT ON FIRM INNOVATION

Introduction

Firms are facing increasing security threats to their information assets. To address these threats, firms in many industries are choosing to appoint a Chief Information Security Officer (CISO), who is charged with mitigating the impact of digital risks on the firm's information security, infrastructure, and relationships with business partners (Kappelman et al., 2020; Maynard et al., 2018). Recent anecdotal evidence suggests that there is a growing trend towards elevating the CISO position as part of the top management team (TMT).[1] The limited existing research on CISOs in TMT relies on qualitative fieldwork to understand CISO legitimacy, particularly from interactions with the board and other TMT members (e.g., Vance et al., 2022). In addition to such internal factors, studies examining other TMT members suggest environmental pressures are important determinants of TMT appointments (e.g., Bendig et al., 2022, Firk et al., 2021, Nath & Mahajan, 2008). However, there are no empirical studies that examine why firms appoint CISOs to their TMT, especially from the perspective of the external environment. Therefore, we pose our first research question: *How does the security behavior and performance of industry peers influence the focal firm's CISO presence in TMT?*

---

[1] Source: https://www.coalfire.com/insights/news-and-events/press-releases/new-coalfire-report-reveals-cisos-rising-influence

Given that most boards view information security as a cost center, the role of CISOs in creating value for the firm remains a challenge for many CISOs seeking to legitimate their place on the TMT. Although risk is associated with innovation (Arend et al., 2017), we know little about how CISOs in TMT contribute to risk management and thereby have a spillover effect on firm innovation. Intuitively, the primary responsibility of the CISO is to limit risk, and thus should constrain innovation. However, the presence of CISOs in TMT could enhance firm innovation through early risk management (Keizera et al., 2002), the introduction of IT products that facilitate access to external knowledge and resources (Lin & Chen, 2012), and a more secure environment (Clò et al., 2020). Therefore, our second research question is: *How does CISO presence in TMT affect firm innovation?*

Since prior experience shapes job performance (Dokko et al., 2009), the type of background and experience of the CISO is likely to moderate the effect of CISO presence on innovation. The upper echelon literature suggests a trade-off between generalists and specialists as executives (Custódio et al., 2013), which can be extrapolated to the CISO context, i.e., a specialist is a CISO with more experience in the same industry of the focal firm (specialist CISO), while a generalist refers to a CISO with more experience in different industries (generalist CISO). On the one hand, industry-specific security regulations-such as the Health Insurance Portability and Accountability Act (HIPAA) in the healthcare industry and the Gramm-Leach-Bliley Act (GLBA) for financial institutions-and the difficulty of transferring industry-specific knowledge can make a specialist CISO in TMT more valuable. In addition, because of their familiarity with the industry, specialist CISOs in TMT may be better positioned to align security policies with business operations and strategies (Wagner & Meshtaf, 2016). Thus, specialist CISOs in TMT may benefit from reduced learning curves in security-business alignment and regulations, allowing other TMT members to make more informed decisions in balancing risks and benefits. On the other hand, literature has demonstrated the advantages of generalists in applying diverse knowledge sets (Custódio et al., 2019). Similarly, generalist CISOs in TMT can bring existing knowledge from other domains to the focal firm, providing alternative perspectives and thus improving innovation. Therefore, we propose our third research question: *How does the type of industry experience of the CISO (i.e., specialist vs. generalist) in TMT differentially affect firm innovation?*

In addition, the influences of CISOs' industry experience on innovation may depend on the competitive environment of the industry. The performance of generalists and specialists depends on the pace of change in their knowledge domain (Teodoridis et al., 2019). Accordingly, we focus on industry turbulence, which refers to the unpredictability of relationships between customers and competitors and the evolution of the market environment (Messersmith et al., 2014; Mithas et al., 2013). Industries with different levels of turbulence have different information flows, security risk profiles, and rates of change, thus moderating the impact of CISO industry experience on firm innovation. Thus, our final research question is as follows: *How does industry turbulence moderate the effects of industry experience of CISOs in TMT on firm innovation?*

We used longitudinal data on S&P 1500 firms from 2008-Q1 to 2020-Q3 to test our hypotheses. We collected data from multiple sources, including BoardEx, Compustat, KPSS, USPTO, Audit Analytics, and LinkedIn. Our results show that industry peers' CISO appointments in TMT and their data breaches are positively associated with the focal firm's CISO presence in TMT. We also find that firms with a CISO in TMT have better innovation performance (in terms of number of patents) than firms without a CISO in TMT. Examining the role of a CISO's prior industry experience, we found that firms with a specialist CISO in TMT can increase innovation by 14.7% more than firms without a CISO in TMT, and by 11.2% more than firms with a generalist CISO in TMT. While we did not find a direct effect of having a generalist CISO in TMT (compared to firms without a CISO in TMT), we did find that the effect of having a generalist CISO in TMT on firm innovation is contingent on industry turbulence, such that firms with generalist CISOs in TMT have better innovation performance than firms without a CISO in TMT in less turbulent industries.

We conducted additional analyses that provided more granular insights into the impact of CISO educational background. The presence of a CISO with an IT and business education in the TMT increases firm innovation by 12.1% and 13.3%, respectively, compared to the presence of a CISO with other backgrounds in TMT. We did not find a significant difference in innovation for firms with a CISO with a law, criminology, or STEM educational background in TMT compared to other firms.

This research is the first to empirically examine the presence of CISOs in TMT and offers theoretical implications for the literature on IT leadership, information security, and firm innovation. Specifically, our findings illustrate the business value of firms appointing CISOs to TMT, which distinguishes our work from prior literature focusing on the security impact of CISOs. We extend prior literature on CISO legitimacy by showing how the security actions of industry peers affect the focal firm's CISO presence in TMT. By illustrating how different CISO backgrounds, such as prior industry experience and educational background, affect firm innovation, we provide insights for managers seeking to develop a profile for hiring CISOs to improve firm security and innovation performance.

Literature Review

Digital Upper Echelons and Firm Innovation

Upper echelons theory focuses on how TMT members affect firm performance (Hambrick & Mason, 1984). Among TMT members, information systems (IS) research has a keen interest in the digital upper echelon, defined as TMT members whose primary portfolios include technology-related responsibilities. For example, the chief information officer (CIO) and chief technology officer (CTO) manage internal IS functions and align them with the business (Carter et al., 2011). Existing research examines how the CIO and CTO shape the formulation and execution of business and IT strategies. Such research suggests that CIO characteristics such as education, age, and tenure are associated with IT-based innovation (Dawson et al., 2016). Research has also shown that the presence of a CIO in the TMT not only improves the financial and operational performance of the firm (Karahanna & Preston, 2013), but also reduces the occurrence of data breaches (Haislip et al., 2021) and positively affects the firm's response to and recovery from data breaches (Zafar et al., 2016).

Digitization has led to new members of the digital upper echelon, whose responsibilities extend beyond the CIO or CTO roles to better capitalize on the opportunities and mitigate the risks associated with digital transformation. For example, firms hire chief digital officers to navigate digitalization (Tumbas et al., 2018) and created CISO positions to mitigate the most worrisome cybersecurity concerns (Kappelman et al., 2020).

With the emergence of digital upper echelons, there is evidence that their presence influences firm innovation in several ways. First, CIOs (Watts & Henderson, 2006) and chief technology innovation officers (Tumbas et al., 2018) can create innovative IT environments. Second, digital upper echelons sometimes lead innovation initiatives and thus directly drive innovation in the firm. For example, the chief data officer's experimenter archetype, which focuses on collaborating with external suppliers and industry peers to explore unidentified markets, can drive firm growth by identifying innovation strategies through big data (Lee et al., 2014). Part of the chief digital officer's responsibility is to lead the company's product innovation (Tumbas et al., 2018). In summary, the digital upper echelon can drive innovation by creating an innovative environment and leading innovation initiatives.

Despite previous research examining the relationship between the digital upper echelons and firm innovation, there is one key difference between CISOs and the rest of the digital upper echelon: focus. Unlike other members of the digital upper echelon whose roles are related to innovation (e.g., leading innovation initiatives or creating an innovative environment), CISOs are not directly tasked with innovation activities. CISOs actively manage the firm’s information security risks, and any spillover from such actions can affect the firm's innovation. Simply put, CISOs oversee the information security risk that is adjacent to or created by firm innovation. Therefore, examining the impact of CISO presence in TMT on firm innovation can enrich the existing literature by demonstrating how security management activities contribute to the link between the top management and firm innovation.

Of all digital upper echelon members, CISOs may be most aware of the security risks associated with innovation. The CISO position requires knowledge of information security risk management and operations, as well as physical and network security (Fitzgerald, 2007). This knowledge depends on CISOs working with other members of the TMT, such as the CEO and CIO, as well as employees (Fitzgerald, 2007) to understand how technology enables the flow of information inside and outside the firm. Although the CISO's knowledge base is highly related to the threats posed by innovation, such as security and risk, studies have not yet examined how CISO presence in TMT affects firm innovation.

Antecedents of Upper Echelon Presence in TMT

Taking an upper echelon perspective, prior literature has examined factors leading to firms' designation of various emerging upper echelon positions in the TMT, such as CIO (Bendig et al., 2022), chief digital officer (Firk et al., 2021), chief supply chain officer (Roh et al., 2016), chief marketing officer (Nath & Mahajan, 2008), and chief strategy officer (Menz & Scheef, 2014). These studies have identified firms' internal strategic (e.g., diversification, alliances, acquisitions, differentiation, strategic fit) and structural (e.g., TMT independence, TMT experience, firm size) factors, as well as external environmental characteristics (e.g., industry concentration, industry IT intensity, threat of new entrants) as important antecedents of the presence of emerging upper echelons in TMT. Recent studies have begun to examine the role of CISOs. For example, Vance et al. (2022) examines how the virtuous cycle of CISO legitimacy to TMT and board members. However, little has been done to understand firms' decisions about CISO presence in TMT, especially from the perspective of the external environment. Thus, in this research, we examine how two types of environmental pressures, i.e., industry peers' CISO presence in TMT and data breaches, influence a focal firm's CISO designation in TMT.

Hypothesis Development

Antecedents of CISO Presence in TMT

The strategy literature has argued that firms in the same industry imitate each other's actions (e.g., Marquis & Tilcsik, 2016), which can be extrapolated to the context of CISO appointments in the TMT. First, firms in the same industry may have similar information security risks. If more industry peers have CISOs in the TMT, the focal firm is more likely to perceive the need to hire a CISO in its TMT to address similar information security concerns. In addition, firms need to be legitimate in the eyes of external stakeholders. When more peers in the same industry have CISOs in the TMT, it becomes an industry norm in the eyes of stakeholders. Thus, due to legitimacy forces, the focal firm is more likely to appoint a CISO in TMT if more industry peers have done so.

Second, competitive forces can explain the within-industry imitation of CISO presence in TMT. Specifically, firms in the same industry often actively engage in competitive actions and reactions (e.g., Livengood & Reger, 2010). Being an early adopter of having a CISO in TMT can help the firm gain competitive advantage (Huang et al., 2014). For example, having a CISO in TMT can help firms differentiate themselves from their competitors by signaling their commitment to protecting sensitive information and ensuring the privacy and security of their customers. This can build trust with customers and translate into increased revenue and market share. To counteract the competitive advantage that industry peers seek from CISO roles in TMT, the focal firm will be more likely to appoint a CISO in TMT. Therefore, we hypothesize that:

Hypothesis 1 (H1). The presence of a CISO in TMT in peer firms is positively associated with the presence of a CISO in TMT in focal firm.

Data breaches at peer firms in the same industry can focus the attention of the focal company and its investors on information security concerns. Because firms in the same industry often have similar business practices and use similar information systems and infrastructure, they may have similar information security risks. In addition, hackers can easily scale their exploitation of vulnerabilities and launch attack programs across firms with similar security risks. In response to the occurrence of data breaches at peer companies, firms are likely to prioritize information security management and, accordingly, are more likely to appoint a CISO to TMT to oversee security responsibilities and budget.

In addition, the increased incidence of data breaches among industry peers increases the firm's perception of security threats in the industry environment. Previous studies have shown that firms are likely to appoint a domain-specific senior executive in TMT in response to threats in the external environment (Firk et al., 2021). Similarly, the firm will be more likely to appoint a CISO in TMT to address the security threat in the external environment when more industry peers experience data breaches. Moreover, from an investor perspective, the occurrence of data breaches among industry peers may increase investor concerns about the focal firm's information security risks (D'Arcy & Basoglu, 2022). Accordingly, the firm's appointment of a CISO in the TMT in response to the increasing number of data breaches in the industry may alleviate investors' information security concerns. Therefore, we hypothesize that:

Hypothesis 2 (H2). The occurrence of data breach in peer firms is positively associated with the presence of a CISO in TMT in focal firm.

CISO Presence in TMT and Firm Innovation

CISOs in TMT advocate paying attention to information security, securing key security resources such as the security budget (Kappelman et al., 2020), and prioritizing security programs (Vance et al., 2022). CISOs in TMT play two important roles. First, they lead the formulation and implementation of the firm's information security strategy (Karanja, 2017). In particular, CISOs in TMT are responsible for assessing IT security threats and their cost significance (Neville-Neil, 2019). Accordingly, the CISO in TMT designs and implements strategies to address identified threats, clarifies the impact of threats that may not be fully mitigated, and prepares firms for threats that emerge in the environment.[2]

Second, CISOs in TMT communicate security knowledge to other TMT members (Maynard et al., 2018). Specifically, CISO presence in TMT increases TMT members' awareness of information security risks through direct communication, thereby influencing their understanding of risk and how it affects the allocation of firm resources. For example, when implementing strategic initiatives, the CISO serves as a "go-to" person for TMT members with IT security concerns related to changing business

[2] Source: Guy Daubenspeck – Kasasa: 'Cybereason CISO Interview Series: Why including information security from a project's start keeps everyone happy.' *Cybereason,* https://www.cybereason.com/blog/blog-cybereason-ciso-interview-series-why-including-information-security-from-a-projects-start-keeps-everyone-happy

processes, markets, or technologies. In these roles, CISOs in the TMT act as business process enablers or facilitators, setting boundaries for TMT members' understanding of information security threats and providing corresponding solutions to mitigate firms' threats (Shayo & Lin, 2019).

Accordingly, we theorize three important ways in which CISO presence in TMT can lead to positive spillover effects on firm innovation: (1) informing other TMT members about the security risk of an innovation project, (2) ensuring the adoption of innovative technologies and applications to better access external resources, and (3) creating a more secure environment, as discussed below.

First, CISO in TMT can assess the firm's security risk and help other TMT members make informed risk decisions regarding the use of innovation enabling IT systems. The presence of CISO in TMT can inform other TMT members about security risks and transform unknown security risks (uncertainty) into known ones, which can promote firm innovation (Osborne & Flemig, 2015). Moreover, risk is embedded in the innovation process. Rather than avoiding risk, early diagnosis and management of risk can help the firm innovate better (Keizera et al., 2002). A stereotype of CISOs is that they tend to reject all risky innovation projects. In practice, however, the CISO in TMT often helps the firm diagnose the security risk and inform other TMT members at an early stage. For example, Johnson & Johnson's CISO claims that the CISO cannot kill the projects, but informs the firm's assessment of the projects through security diagnosis and offers an appropriate strategy to reduce the security risk. This early diagnosis of security risk can help the firm manage security risk while engaging in innovation activities, which can help improve the success of innovation projects.

"In our companies it's all about risk and what we need to have is what is our cyber risk posture for different areas of our business … I'm not gonna tell my business don't do business in X, Y, Z country. I'm going to explain to them. Okay if you're going to do business in this country, then we will need to put these type of things in and you're gonna have a limitation. Your data is not private. They have the right to those keys, the data of their country, of their citizenship, is not allowed to leave. This could create implications in their build-up and their business and as long as you're very up front with that."
– Marene Allison, CISO at Johnson & Johnson, 2020[3]

Second, the presence of the CISO in the TMT may convince the firm to adopt IT systems and tools that may be considered risky but could significantly improve the collaboration and productivity of the research and development (R&D) team. For example, many emerging technologies such as cloud computing and big data analytics have significant impact on the innovation efficiency and outcomes of firms (Lin & Chen, 2012). However, information security remains a top concern that makes firms reluctant to adopt these technologies (Yang et al., 2017). The presence of a CISO in TMT can strategically assess and control security risks, establish secure usage procedures, and clearly communicate related issues, thereby reducing the security barriers to using new technologies to improve innovation. In another example, the CISO at Illumina explicitly articulated a similar case of facilitating the company's adoption of Wi-Fi, which improves employees' access to external resources and knowledge critical to innovation.

"*…I was once Head of Security and IT Operations at a financial institution that didn't have wireless networking. This was some years ago, but it was a time when most businesses had a wireless network. I asked leadership why they didn't have one and they said, "Well, the auditors really frowned upon it and there was a lot of questions." Then they said, "And frankly, we haven't had the time to figure out how to secure it*

[3] Source: Marene Allison - Johnson&Johnson: 'CISO 500 Interviews. Security In Healthcare. Marene Allison, CISO, Johnson & Johnson.' *CyberCrime Magzine.* https://soundcloud.com/cybercrimemagazine/ciso-500-marene-allison-vp-ciso-at-johnson-johnson

properly." At that, I just thought it was entirely their job to have had that basic tool. I realized I couldn't cop out on that responsibility and that was obviously an easy win for me, just to bring wireless to an organization."
– Jason Callahan, chief information security officer at Illumina, 2018[4]

Third, CISO presence in TMT can create a more secure environment that fosters innovation development processes. Given the responsibilities and security budget benefits of the CISO in TMT as elaborated above, firms with CISO presence in TMT are more likely to build safer environments with lower and known information security risks than other firms in the same industry without CISO in TMT. Innovation literature has identified different types of "safer environments" in terms of job security and institutional security that influence the firm's innovativeness (e.g., Clò et al., 2020). Given the growing concern about data breaches, a safe environment in terms of information security is likely to influence firm innovation. For example, firms' innovation projects often contain sensitive information, i.e., information breaches in innovation projects can lead to the leakage of business secrets and core competitive technologies. By providing a more secure environment for R&D, the presence of CISOs in TMT may alleviate knowledge creators' concerns about information security and allow them to focus their efforts on value-creating activities, leading to greater innovation. Therefore, we hypothesize that:

Hypothesis 3 (H3). CISO presence in TMT is positively associated with a firm's innovation.

---

[4] Source: Jason Callahan – Illumina: 'Cybereason CISO Interview Series: Security's appeal lies in the challenge.' *Cybereason,* https://www.cybereason.com/blog/cybereason-ciso-interview-series-jason-callahan-illumina

Impact of CISO Industry Experience

The impact of CISO presence in TMT on firm innovation (i.e., H3) may depend on the prior experience of the CISO. Accordingly, we categorize CISOs into two groups: (1) a specialist CISO who has more work experience in the same industry as the focal firm, and (2) a generalist CISO who has more work experience in industries different from the focal firm. We chose industry as the boundary of CISO experience because it is commonly used to define competitive and regulatory boundaries (Meyer et al., 1990). We consider the context of IT security and industry boundaries in our theorization of the effects of different CISO types. We contend that the positive impact of CISO in TMT on firm innovation is greater when the presence of CISO with more experience in the same industry in TMT. In other words, we predict that firms with specialist CISOs in TMT will innovate more than those with no CISO in TMT, but that there will be no difference in innovation between firms with generalist CISOs in TMT and those with no CISO in TMT. We discuss these arguments in more detail below.

Because of the similarity in business and security risk profiles among firms in the same industry, specialist CISOs in TMT can apply relevant knowledge gained from work experience or learned from peers in the same industry, thereby enhancing the mechanisms (theorized in H3) of how CISOs facilitate innovation. In contrast, generalist CISOs who lack industry-specific knowledge may have difficulty triggering these mechanisms.

First, specialized CISOs in the TMT could use their deep contextual knowledge to provide more effective early diagnosis of security risks and communicate them to senior management in an efficient manner. CISOs often develop industry-specific security strategies to align with the ins and outs of the business. In other words, CISOs in different industries are likely to have heterogeneous concerns and practices when it comes to securing customer information. For example, one reason healthcare data is vulnerable is the delay between outpatient and insurance verification, so CISOs in healthcare organizations will likely focus their protection strategies on this delay. Financial institutions, on the other hand, are under pressure to complete transactions more quickly, requiring near real-time verification. Although both healthcare and financial institutions deal with personal information, the sensitivity of different types of information is not quite the same. As a result, specialist CISOs in the TMT industry can leverage their experience in the same industry to quickly identify the security focus and apply strategies that are consistent with industry norms, thereby better fulfilling their responsibilities. In contrast, generalist CISOs in TMT may assess security threats and develop security strategies based on the common security practices of other industries in which they have worked (i.e., commonly known as behavioral inertia), leading to more trial and error and hindering their positive impact on innovation.

Beyond efficient evaluation of security risk, specialist CISOs in TMT would presumably have advantages in communications with other TMT members and employees because of their industry-specific business knowledge, which facilitates the firm's knowledge discovery and integration, thereby improving innovation. Specifically, prior work experience in the same industry would be expected to increase the CISO's cumulative industry-specific business knowledge. For example, a CISO with rich experience in the healthcare industry would likely be able to better understand how healthcare organizations operate and be more familiar with healthcare-specific jargon relevant to communicating with the TMT than a CISO with experience in the construction industry. Such strong, current industry knowledge can help specialist CISOs in TMT communicate with other TMT members as well as business unit managers. Smooth communication between a specialist CISO in TMT and business managers can enhance knowledge discovery efforts and minimize slow-downs due to security threat assessments, thereby promoting greater firm innovation. In contrast, a generalist CISO in TMT who lacks industry-specific knowledge may encounter difficulties in communicating security concerns to other TMT members, which would negatively impact firm innovation.

Second, specialist CISOs can enable the most appropriate adoption of IT products that can optimize business performance, such as innovation. The similarity of business profiles among companies in the same industry suggests that they may face similar security threats. Specialized CISOs in TMT can adopt security strategies that they or others in the same industry have tested, reducing the cost of trial and error. For example, a CISO with experience in the healthcare industry can easily limit the number of emails an employee sends to a patient to the best rule of thumb. In contrast, generalist CISOs in the TMT may overreact to bogus security alerts, unduly restricting employees and further reducing innovation.

Third, a specialist CISO would be more likely than a generalist CISO to develop the "know-how" to comply with industry-specific security regulations, and thus be better able to assess and control security risks, support valuable tools with previously unknown risks, and create a more secure environment capable of facilitating innovation. In particular, the proliferation of industry-specific information security regulations requires the CISO in TMT to have a good understanding of industry regulatory policies. For example, CISOs in financial institutions are expected to be familiar with the Gramm-Leach-Bliley Act (GLBA), CISOs in healthcare organizations are likely to understand how to comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and CISOs in educational organizations are expected to have a good understanding of the Family Educational Rights and Privacy Act (FERPA). Specialist CISOs tend to have a better understanding of how to comply with industry-specific regulations than generalist CISOs due to their extensive industry experience. With their intimate knowledge of industry regulations, specialist CISOs in the TMT sector are better able to align security with the company's specific business beyond checking the "compliance box" and thus better facilitate innovation. In contrast, generalist CISOs in TMT must invest time in learning to comply with industry regulations, reducing their potential positive impact on business innovation. Thus, we hypothesize that:

Hypothesis 4 (H4). CISO's industry experience moderates the impact of CISO presence in TMT influence on firm innovation. Specifically, the presence of a specialist CISO (i.e., who has more prior experience in the focal firm's industry) in TMT increases firm innovation.

Impact of Industry Turbulence

The disadvantages of generalist CISOs in TMT for firm innovation may manifest in different ways across industries. We propose that industry turbulence alters the relationship between generalist CISO presence in TMT and firm innovation, such that generalist CISO presence in TMT can increase firm innovation in less turbulent industries. Industry turbulence refers to the unpredictability of customer and competitor relationships and trends in the market environment (Messersmith et al., 2014, Mithas et al., 2013). However, in contrast to generalist CISOs in TMT, industry characteristics are unlikely to alter how specialist CISOs in TMT apply their prior experience to the focal firm in promoting innovation. In other words, regardless of turbulent or stable industry environments, specialist CISOs in TMT can apply their prior experience from the same industry to foster firm innovation. Therefore, we focus on the moderating effects of industry turbulence on the impact of generalist CISO presence in TMT on firm innovation, as argued below.

A turbulent industry may exacerbate the disadvantages of generalist CISOs in TMT for several reasons. First, turbulent environments increase uncertainty, which requires a continuous flow of knowledge and information for the firm to survive (Kim et al., 2021). As a result, firms in turbulent industries are expected to deal with greater demands and more volatile information assets (Feng et al., 2021), which requires CISOs in TMT to be familiar with industry-specific information security regulations and business operations to fulfill security responsibilities in a high-quality and efficient manner. Second, volatile information flows in rapidly changing environments increase the complexity of information security risk profiles. Thus, turbulent industry environments require CISOs to have a deeper knowledge of industry practices. Third, turbulent environments require firms to respond to unpredictable market changes (Mithas et al., 2013), which reduces the time and opportunity for the CISO in TMT to explore security strategies and operations through trial and error. Thus, in turbulent industries, the disadvantages of generalist CISOs in TMT in facilitating innovation are likely to be exacerbated.

In contrast, the benefits of generalist CISOs are likely to manifest themselves in less turbulent industries for several reasons. First, business operations and industry environments are more predictable in less turbulent industries, giving generalist CISOs time to become familiar with industry security regulations and risk profiles. Second, in less turbulent environments, CISOs have more latitude to explore information security strategies and operations. Third, in less turbulent industries, the firm’s information flow is less complex and more predictable, making it easier to protect. Thus, generalist CISOs can more easily learn the security practices of their new industry and adapt to their security responsibilities in less turbulent environments, allowing generalist CISOs to migrate their prior knowledge from other industries to the focal firm and facilitating the integration of diverse knowledge. Prior literature suggests that new knowledge outside the focal firm's domain can facilitate innovation (Xiao et al., 2022). Thus, we expect that the presence of a generalist CISO in TMT can enhance firm innovation in less turbulent industries. Therefore, we hypothesize that:

Hypothesis 5 (H5). Industry turbulence moderates the contingent impact of CISO industry experience on firm innovation. Specifically, the presence of a generalist CISO in TMT is positively associated with firm innovation in less turbulent industries.

Figure 2.1 summarizes our research model.

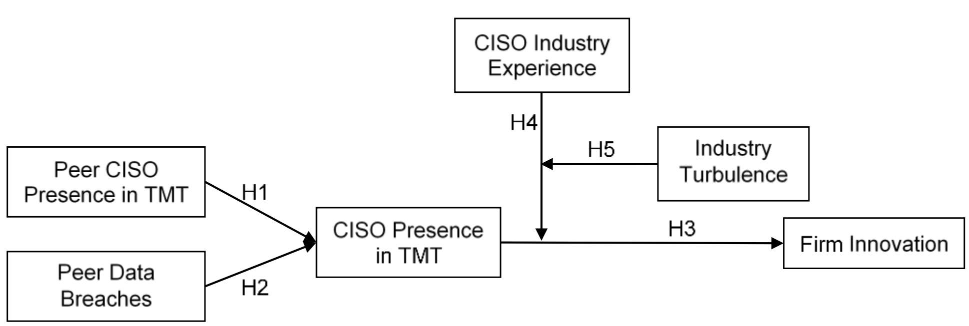

Figure 2.1. The Research Model of CISO Presence in TMT

Method

Data

To empirically test our hypotheses, we collected data on firms listed in the S&P 1500 between 2005 and 2020. The S&P 1500 includes large, medium, and small firms and has been commonly used in prior research on innovation and upper echelons (e.g., Dezsö & Ross, 2012). For each firm in our sample, we collected firm-quarter panel data from several sources. First, we collected patent data for each firm from the KPSS patent database (Kogan et al., 2017), which contains patent filing information for public firms as reported to the United States Patent and Trademark Office (USPTO) through September 2020. Because the USPTO only provides information on patent filings, grant dates, and citations of other patents, we used the patent identifier (i.e., patent_num) from KPSS to merge each patent with the USPTO. Second, we obtained individual-level data on the job titles and job status of each firm's executives from the BoardEx database. Third, we obtained the financial performance of our sample firms from the Compustat database and collected data on industry characteristics based on all public firms. Fourth, we manually collected the educational background of each identified CISO from LinkedIn by searching the names of CISOs and verifying their prior work experience. Fifth, we collected information on corporate data breaches from Audit Analytics and used it to construct our instrumental variables. Audit Analytics provides a comprehensive list of major data breaches at public companies, compiled from SEC filings, press releases, and government documents.[5] We merged the data collected from these sources using common

[5] Refer to https://www.auditanalytics.com/products/sec/cybersecurity for more details about audit analytics.

identifiers.[6] We imputed missing values in the Compustat data. Our final sample includes 70,650 firm-quarter observations from 1,592 firms from 2008-Q1 to 2020-Q3.

Variable Definitions

Variables of Interest

To measure innovation, we used the total number of USPTO-approved patents filed by firm i in quarter t (Xue et al., 2012), denoted $Innovation_{it}$. We used the filing date of the approved patents because patents often take more than 18 months to be approved.[7] We used its natural logarithm form of one plus the number of patents because of its highly skewed distribution and to avoid taking logarithms on zeros.

The variable $CISOTMT_{it}$ refers to whether the firm *i* had a designated executive in TMT overseeing IT security-related issues in quarter *t*, which equals one if it did and zero otherwise. Given inconsistent labeling of CISO positions in companies, we performed a keyword search on all job titles of the public firm senior managers or above in BoardEx. We determined the keywords by manually coding half of the total available unique job titles (N = 1200). Specifically, we matched the keywords "security," "information security," and "chief security" in each manager's job title and description fields to identify CISOs. To restrict our search to security-related managers in TMT, we followed previous literature and included managers at the vice president level or above (e.g.,

---

[6] Although these data sources have different identifiers, we were able to match them using common identifiers appeared in at least two datasets. Specifically, we merged USPTO and KPSS data using *patent_num* at the patent level and aggregated it to the firm-level using KPSS's *permno* column as the unique firm identifier. Then, we merged the data with CRSP using *permno*. Next, we used the *ticker* provided in CRSP as the unique firm identifier to match the data from Compustat and BoardEx. Finally, we leveraged BoardEx's executive name and job experience as the identifier to match the data collected from LinkedIn.

[7] Source: https://www.uspto.gov/dashboard/patents/pendency.html

Guldiken et al., 2019). Specifically, we used the keywords "chief," "officer," "vice president" and "vp" to identify CISOs in TMT. Finally, we manually verified all returned results to ensure accuracy.

We measure $PeerCISOTMT_{it}$ using the average number of CISOs in TMT in firms in the same industry with the focal firm *i* at quarter *t*. We constructed variable $PeerBreach_{it}$ as the average number of data breaches experienced by firms in the same industry with the focal firm *i* at quarter *t*. We measured CISOs' industry experience using the percentage of each CISO's previous jobs in the same industry as their current firm out of their total number of jobs, denoted as the variable *IndustryExperienceRatio*. A larger value of the measure indicates that the CISO has accumulated more experience in their current industry, whereas a smaller value demonstrates that the CISO possesses generalist experience beyond the focal firm's industry. Accordingly, we coded two binary variables to measure the different types of CISOs. Specifically, $SpecialistCISOTMT_{it}$ equals one if the value of $IndustryExperienceRatio_{it}$ for the CISO of firm *i* at year *t* is greater than the variable's sample mean and zero otherwise. In contrast, if the value of $IndustryExperienceRatio_{it}$ for the CISO of firm *i* at year *t* is smaller than the variable's sample mean, we identified the CISO as a generalist CISO and coded the variable $GeneralistCISOTMT_{it}$ as one, coding it as zero otherwise. By doing so, CISOs are categorized as either a specialist or generalist CISO.

We followed Mithas et al., (2013) and measured $IndustryTurbulence_{it}$ using the total number of firms entering and exiting firm *i*'s industry in year *t,* scaled by the industry's total number of firms at the end of the previous year. We used the primary three-digit NAICS code to denote industry, which is commonly used in strategy research (e.g., Honoré, 2022).

Control Variables

We controlled for several factors related to the firm's financial characteristics, industry attributes, and TMT composition because they may affect a firm's designation of a CISO and innovation. First, we included firm-level financial variables used in prior studies (e.g., Mao & Weathers, 2018; Xue et al., 2012). *FirmSize* was measured as the log form of one plus total assets. *Profitability* is the return on assets, which is the ratio of net income to total assets. We measured *Leverage* using the ratio of total debt to total assets. We also controlled for *AssetTangibility*, which is the ratio of plant, property, and equipment to total assets. We included *CapitalExpenditure*, measured as the ratio of capital expenditure to total assets. *FirmAge* was measured as the log form of one plus the number of years the firm has been listed. We controlled for *GrowthOpportunity* using Tobin's q, which measures the market-to-book ratio. The variable *R&DExpenditure* refers to the R&D expenditure scaled by total assets.

Second, we included industry-level variables used in previous studies (e.g., Keats & Hitt, 1988; Mithas et al., 2013; Xue et al., 2011). We defined industry at the primary three-digit NAICS code level, including all listed firms. *IndustryGrowth* was operationalized as the three-year growth in total sales. We controlled for *MarketConcentration* using the Herfindahl-Hirschman index, which is the sum of the square format of each firm's market share in the focal industry (i.e., market share is computed as the firm *i*'s annual sales scaled by focal industry total annual sales).

Third, we controlled for the presence of other relevant TMT members, given their potential impacts on CISO presence and innovation. We controlled for the presence of a chief innovation officer using the variable *CInnOPresence*, which equals one if the firm has a chief innovation officer and zero otherwise. We included the presence of a chief risk officer using the variable *CROPresence*, which equals one if the firm has a chief risk officer and zero otherwise. We also included the variable *TechOfficer* to control for the presence of other digital upper echelon members, which equals one if the firm has a chief information officer, chief technology officer, or chief digital officer, and zero otherwise.

Table 2.1. Descriptive Statistics of CISO Presence in TMT Paper

Variables	Mean	S.D.	Min	Max
Variables of Interest				
Innovation	0.53	1.15	0.00	8.06
CISOTMT	0.08	0.27	0.00	1.00
SpecialistCISOTMT	0.03	0.17	0.00	1.00
GeneralistCISOTMT	0.05	0.21	0.00	1.00
IndustryTurbulence	0.12	0.06	0.00	0.77
Control Variables				
FirmSize	8.14	1.76	0.02	14.99
Profitability	0.01	0.05	-2.84	3.75
Leverage	0.00	0.01	-1.17	1.11
AssetTangibility	0.23	0.24	0.00	0.98
CapitalExpenditure	0.03	0.04	-0.13	0.71
R&DExpenditure	0.01	0.02	0.00	0.49
TechOfficer	0.48	0.50	0.00	1.00
CROPresence	0.13	0.33	0.00	1.00
CInnOPresence	0.05	0.23	0.00	1.00
FirmAge	3.12	0.69	0.00	4.09
GrowthOpportunity	2.13	25.91	0.31	6867.58
MarketConcentration	0.08	0.09	0.01	1.00
IndustryGrowth	0.00	0.03	-0.93	1.64

Note: Number of observations: 70650

Table 2.1 presents the descriptive statistics. Appendix A presents the correlations among all variables. We also ran variance inflation factors (VIFs) to assess multicollinearity. All VIFs are well below 10 (Hair et al., 1995), with the maximum VIF of 1.70, indicating that multicollinearity is not a concern in this study.

Empirical Approach

We used linear fixed-effect models with clustered standard errors to test our hypotheses. The fixed-effect model controls for time-invariant heterogeneity. In addition, we included quarter-fixed effects to control for time-specific unobserved heterogeneity. We estimated the following equation to examine H1 and H2.

$$CISOTMT_{it} = \beta_0 + \beta_1 PeerCISO_{it} + \beta_2 PeerBreach_{it} + \lambda \cdot X_{it} + \alpha_i + \tau_t + \epsilon_{it} \quad (1)$$

where β refers to the coefficients, X_{it} indicates the vector of all time-variant control variables specified in Table 2.1, λ is the coefficient metrics for control variables, α_i indicates firm fixed effect, τ_t indicates quarter fixed effect, and ϵ_{it} is the error term.

To empirically test H3 regarding the overall impact of CISO presence in TMT on firm innovation, we estimated:

$$Innovation_{it} = \beta_0 + \beta_1 CISOTMT_{it} + \lambda \cdot X_{it} + \alpha_i + \tau_t + \epsilon_{it} \quad (2)$$

H4 concerns the different impacts of specialist and generalist CISOs in TMT on firm innovation, compared to firms without a CISO in TMT. Thus, we revised the equation (2) by replacing the binary code of *CISOTMT* variable with a categorical variable including three categories: (1) firms without a CISO in TMT, (2) firms with a specialist CISO in TMT, and (3) firms with a generalist CISO in TMT. Similar to equation (1), when testing H1, we used firms without a CISO in TMT as the baseline.

Thus, we estimated the model with two binary variables of *SpecialistCISOTMT* and *GeneralistCISOTMT*, as shown in the following equation. The significance of coefficients on *SpecialistCISOTMT* and *GeneralistCISOTMT* demonstrate the specialist and generalist CISOs in TMT' impacts on firm innovation, compared to firms without a CISO in TMT.

$$Innovation_{it} = \beta_0 + \beta_1 SpecialistCISOTMT_{it} + \beta_2 GeneralistCISOTMT_{it} + \lambda \cdot X_{it} + \alpha_i + \tau_t + \epsilon_{it} \text{ (3)}$$

To empirical test H5, we added the interaction term between industry turbulence and the presence of different types of CISOs in TMT to Equation (3). Specifically, we estimated:

$$Innovation_{it} = \beta_0 + \beta_1 SpecialistCISOTMT\ _{it} + \beta_2 GeneralistCISOTMT\ _{it} + \beta_3 SpecialistCISOTMT_{it} \times IndustryTurbulence_{it} + \beta_4 GeneralistCISOTMT_{it} \times IndustryTurbulence_{it} + \beta_5 IndustryTurbulence_{it} + \lambda \cdot X_{it} + \alpha_i + \tau_t + \epsilon_{it}$$
(4)

where β_4 is the coefficient of interest, X_{it} is the vector of all time-variant control variables specified in Table 2.1, λ is the coefficient metrics for control variables, α_i indicates firm fixed effect, τ_t indicates quarter fixed effect, and ϵ_{it} is the error term.

Results

We first examined the results of our baseline models. We then addressed the endogeneity concern using the two-stage least square (2SLS) model. We also empirically tested the theorized mechanisms and ruled out alternative explanations. Further, we conducted post-hoc analyses to enrich our findings and ran additional robustness checks to ensure the results' stability. Table 2.2 summarizes our empirical analyses.

Table 2.2. Summary of Empirical Analyses

Empirical Analysis	Results	Location
1. Baseline model for hypothesis testing	All hypotheses are supported	Table 2.3
2. Addressing endogeneity concern of CISO presence in TMT and firm innovation using 2SLSe estimation	Consistent results	Appendix B
3. Testing mechanisms of CISO presence in TMT's impacts on firm innovation		
3.1 Use TMT's risk-seeking incentive to test the mechanism that CISO presence in TMT boosts innovation through better communication with TMT members on security risks	Supported	Appendix C
3.2 Use the firm's commitment to IT to test the mechanism that CISO presence in TMT boosts innovation by facilitating the adoption of IT products that improve access to external resources and knowledge	Not supported	Appendix C
3.3 Use the firm's security awareness to test the mechanism that CISO presence in TMT increases innovation through improving the security of environment	Supported	Appendix C
4. Falsification tests to ensure the results are driven by CISO presence in TMT		
4.1 Use middle-level information security manager's presence to ensure the results are driven by CISO's presence in TMT instead of other security managers	Presence of middle-level information security manager doesn't affect firm innovation	Appendix D
4.2 Use CISO turnover to ensure the results are driven by CISO's presence in TMT instead of previous CISOs	CISO turnover reduces firm innovation	Appendix D
5. Post-hoc analyses on the impacts of CISOs' educational background	CISOs with business and IT background in TMT have stronger positive impacts on firm innovation	Appendix E
6. Additional robustness checks		
6.1 Alternative definition of industry boundary	Consistent results	Appendix F

Table 2.2. (continued)

Empirical Analysis	Results	Location
6.2 Alternative threshold of specialist versus generalist CISO	Consistent results	Appendix F

Results of Hypothesis Testing

Table 2.3 reports the results of hypothesis testing. As shown in Column (1) in Table 2.3, the coefficients on both *PeerCISOTMTs* ($\beta = 0.190$, $p < 0.1$) and *PeerDataBreaches* ($\beta = 0.342$, $p < 0.05$) are statistically significant when predicting *CISOTMT*, indicating that industry peers' CISO presence in TMT and data breaches are positively associated with the focal firm's CISO presence in TMT. Hence, H1 and H2 are supported. As shown in Column (2) in Table 2.3, the coefficient of *CISOTMT* is positive and significant ($\beta = 0.080$, $p < 0.05$), indicating that firms with a CISO had an 8% higher approved patent count, on average, than those without a CISO. Thus, H3 is supported.

Column (3) in Table 2.3 demonstrates that the presence of specialist CISO in TMT positively and significantly influences firm innovation ($\beta = 0.147$, $p < 0.05$). On average, firms with specialist CISOs in TMT had about 14.7% more approved patents than those without CISO presence in TMT. However, the presence of generalist CISOs in TMT did not significantly influence firm innovation ($\beta = 0.045$, p = n.s.), which also confirms our theoretical motivation to examine the moderating effects of industry turbulence. Therefore, H4 is supported. We also empirically compared the innovation impacts of specialist and generalist CISOs in TMT by using the presence of generalist CISOs in TMT as the baseline and using only data from a subsample of firms that have a CISO in TMT. As shown in Column (4) in Table 2.3, the coefficient on the presence of

Table 2.3. Results of CISO Presence Hypothesis Testing

Variables	**(1)** *CISOTMT*	**(2)** *Innovation*	**(3)** *Innovation*	**(4)** *Innovation*	**(5)** *Innovation*
PeerCISOTMT	0.190* (0.109)				
PeerBreach	0.342** (0.167)				
CISOTMT		**0.080**** **(0.039)**			
WithoutCISOTMT		Baseline	Baseline	-0.148*** (0.055)	Baseline
SpecialistCISOTMT			**0.147**** **(0.060)**	**0.112*** **(0.061)**	0.172** (0.076)
GeneralistCISOTMT			0.045 (0.042)	Baseline	0.166*** (0.063)
SpecialistCISOTMT × IndustryTurbulence					-0.205 (0.552)
GeneralistCISOTMT × IndustryTurbulence					**-0.945**** **(0.424)**
IndustryTurbulence		0.252*** (0.093)	0.253*** (0.094)	0.152 (0.341)	0.309*** (0.104)
FirmSize	0.011 (0.007)	0.084*** (0.018)	0.085*** (0.018)	0.156** (0.071)	0.085*** (0.018)
Profitability	-0.028 (0.019)	-0.087 (0.062)	-0.086 (0.061)	-0.116 (0.352)	-0.084 (0.061)
Leverage	-0.009 (0.006)	0.151*** (0.028)	0.151*** (0.028)	16.872 (56.836)	0.154*** (0.028)
AssetTangibility	-0.000 (0.037)	0.241** (0.094)	0.241** (0.094)	0.354 (0.346)	0.238** (0.094)

Table 2.3. (continued)

Variables	(1) *CISOTMT*	(2) *Innovation*	(3) *Innovation*	(4) *Innovation*	(5) *Innovation*
CapitalExpenditure	0.057*	-0.046	-0.049	0.091	-0.042
	(0.032)	(0.090)	(0.090)	(0.404)	(0.090)
R&DExpenditure	-0.032	2.171**	2.181**	1.593	2.185**
	(0.274)	(0.848)	(0.849)	(1.276)	(0.848)
TechOfficer	-0.222***	0.042***	0.042***	0.125**	0.042***
	(0.014)	(0.015)	(0.015)	(0.054)	(0.015)
CROPresence	0.030**	0.006	0.007	-0.027	0.006
	(0.014)	(0.024)	(0.024)	(0.061)	(0.024)
CInnOPresence	0.030**	-0.002	-0.003	0.056	-0.005
	(0.015)	(0.036)	(0.036)	(0.062)	(0.036)
FirmAge	0.033*	0.167***	0.165***	0.187	0.166***
	(0.019)	(0.035)	(0.035)	(0.116)	(0.035)
GrowthOpportunity	0.000*	0.000**	0.000**	-0.019	0.000**
	(0.000)	(0.000)	(0.000)	(0.023)	(0.000)
MarketConcentration	0.063*	-0.142	-0.152	-0.817	-0.162
	(0.038)	(0.218)	(0.217)	(0.680)	(0.217)
IndustryGrowth	-0.044	0.079	0.078	-0.107	0.075
	(0.108)	(0.077)	(0.077)	(0.267)	(0.077)
Firm Fixed Effects	Yes	Yes	Yes	Yes	Yes
Quarter Fixed Effects	Yes	Yes	Yes	Yes	Yes
Number of Observations	70650	70650	70650	12635	70650
R^2	0.196	0.106	0.107	0.189	0.107

Notes: Significance levels: *p < 0.1, **p < 0.05, ***p < 0.01; Clustered standard errors are in parentheses.

specialist CISOs in TMT is positive and significant (β = 0.112, $p < 0.1$), demonstrating that the presence of a specialist CISO in TMT has a stronger impact on firm innovation than the presence of a generalist CISO in TMT.

As shown in Column (5) in Table 2.3, the coefficient on the interaction term between generalist CISO in TMT and industry turbulence is negative and significant (β = -0.945, $p < 0.05$), indicating that industry turbulence weakens the positive impact of the presence of a generalist CISO in TMT on firm innovation. Specifically, generalist CISOs in TMT are positively associated with firm innovation when the industry turbulence is low but negatively associated with firm innovation when the industry turbulence is high. Hence, H5 is supported. Results in Column (4) also indicate an insignificant coefficient on the interaction between specialist CISO in TMT and industry turbulence (β = -0.205, p = n.s.), confirming our theoretical prediction that the impact of specialist CISOs in TMT on firm innovation is not contingent on industry turbulence.

Addressing Endogeneity Concerns

Although we controlled for factors related to industry, firm, and TMT characteristics, identification may be biased due to potential unobservable omitted variables. For example, firms with higher IT investments are more likely to appoint a CISO in the TMT, while they tend to have higher levels of innovation due to high IT innovativeness. Therefore, we used an instrumental variable approach to mitigate endogeneity concerns and estimated the 2SLS model. Ideal instruments would be expected to significantly influence firms' CISO presence in TMT, but not directly influence firms' innovation.

In research, the behaviors and outcomes of industry peers have been commonly used as instruments of the focal firm's strategic actions (Nath & Bharadwaj, 2020). Similarly, *PeerCISOTMT* and *PeerBreach* would qualify as ideal instrumental variables for a focal firm's CISO presence in TMT. Specifically, we have theorized and empirically validated the impact of industry peers' CISOs in TMT and data breaches on the focal firm's CISO presence in TMT. However, industry peers' CISOs in TMT and their data breaches are unlikely to directly influence the focal firm's innovation outputs.

We used *xtivreg2* in the Stata software package to execute the 2SLS model and check the qualifications of the instrument variables. We performed a weak identification test using Cragg-Donald Wald F statistic ($F = 44.14$), which is much larger than the 10% maximal relative bias of the Stock-Yogo weak identification test critical value, i.e., 19.93, thus satisfying the first-stage relevance assumption of instrument variables. To assess overidentification, we relied on the Hansen-Sargan test. Results show that the Hansen J statistic ($\chi^2_{(1)} = 0.001$) is insignificant ($p = 0.9901$), validating the overidentification restrictions of instruments. As shown in Appendix B, the second-stage regression results indicate that *CISOTMT* has a positive and significant influence on firm innovation ($\beta = 4.842$, $p < 0.05$), which is consistent with our main hypothesis test results.

Mechanisms

We develop proxy measures to empirically test the hypothesized mechanisms explaining how CISO presence in TMT affects firm innovation. First, we use the risk-taking incentives of the TMT to test the theorized mechanism that CISO presence in the TMT promotes innovation through better communication with TMT members about security risks. The intuition is that the TMT with higher risk-seeking incentives will have less need to transform unknown risks into known ones. In other words, the TMT with higher risk-taking incentives is more likely to support risky innovation projects and activities and is less influenced by whether the risks are known and certain. Accordingly, the positive impact of CISO presence in the TMT on innovation should be weakened because their assessment of security risk is less considered in the innovation decision process. We collected additional data from CRSP, ExecuComp and Federal Reserve System. We measure the TMT's risk-taking incentives using the average of each executive's *Vega*, which is the change of the executive's option portfolio given changes with a 0.01 unit increase in the stock return's annualized standard deviation (Coles et al., 2006). Appendix C provides the details about the calculation of *Vega*. As shown in Column (1) in Appendix C table, the TMT's risk-taking incentives weaken the positive impact of CISO presence in TMT on firm innovation, therefore supporting our proposed mechanism.

Second, we use the firm's commitment to IT to test our hypothesized mechanism that the presence of CISOs in TMT enhances firm innovation by facilitating the adoption of IT products that improve access to external resources and knowledge. The firm's commitment to IT indicates the managerial attention and resources allocated to IT (Engelen et al., 2022). We expect that the effect of CISO presence in TMT on firm innovation will be attenuated if the firm already has a higher commitment to IT. This is because firms with a higher commitment to IT are more likely to introduce innovative IT products than firms with a lower commitment to IT. These innovative IT products introduced in firms with higher commitment to IT exhaust the IT products that have access to external resources or knowledge that can be further introduced by the CISO in

TMT. We measured commitment to IT using changes in the frequency of IT-related keywords appearing in the company's SEC quarterly report. We used the keywords developed by Engelen et al. (2022). Column (2) of Table C1 shows an insignificant coefficient on the interaction term between CISO presence in TMT and firm commitment to IT. Thus, the second mechanism is not supported. A possible explanation is that the adoption of IT products depends on the activities of CIOs rather than CISOs. Thus, the impact of CISOs on IT products that have external resources and knowledge is limited.

Third, using security awareness as a proxy measure for the security environment of firms, we test the third mechanism that CISO presence in TMT will increase innovation by improving the security of the firm's environment. We argue that the positive effect of CISO presence in TMT on firm innovation is attenuated by higher security awareness. This is because when overall security awareness in the firm is relatively low, the CISO in TMT can help improve the security environment for employees to protect their innovation creation process. However, when security awareness is high, there is less room for the CISO to improve the security of the organization's environment. We measured security awareness using changes in the frequency of security-related keywords in the company's quarterly SEC filings. We used the security-related keywords identified in D'Arcy & Basoglu (2022) and Li et al. (2023). As shown in Column (3) of Table C1, security awareness weakens the positive impact of CISO presence in TMT on firm innovation, supporting our proposed mechanism.

Falsification Tests

We ran falsification analyses to ensure the identified impacts on innovation are mainly driven by CISO presence in TMT. First, we ensure that the effects are bounded to

CISO presence in *TMT* instead of middle-level information security managers. We constructed a variable *MidSecManager* to denote firms that have information security manager only at the middle manager level, i.e., no security manager in TMT. We manually coded the title of security managers and found 495 out of 737 middle security managers have previously worked in firms that only have middle-level information security managers at the highest level and have no CISO in TMT. As shown in Column (1) in Appendix D, the presence of only middle-level information security managers has an insignificant impact on firm innovation ($\beta = -0.016$, p = n.s.), confirming that our results are specific to CISO in TMT. In other words, appointing information security managers at the middle-level does not affect firm innovation.

Second, to demonstrate that the identified impacts are driven by CISO *presence* in TMT, we tested whether the turnover of the CISO in TMT reduced the firm's innovation. CISO in TMT's turnover presumably reduces innovation because security policy is dynamic and requires firm knowledge to adjust it to fit the industry environment (Karyda et al., 2005). Also, firm knowledge is required to effectively maintain security systems. CISO in TMT's turnover would be expected to negatively impact innovation by creating incompatible systems and unsuitable policies in the long run. Since in the short run, both policies and systems are still compatible with the firm and can operate without major maintenance efforts, the diminishing impact may not take effect immediately. We measured CISO in TMT's turnover as a dummy variable, which equals one if the CISO in TMT's turnover occurred in the past year (i.e., four quarters). We replaced the main independent variable with the turnover measure, denoted as *CISOTMTTurnover*, and reran the model. We also ran models with different CISO in TMT's turnover windows (i.e., five to eight quarters). As shown in Columns (2)-(6) in Appendix D, CISO in TMT's turnover had a negative and significant impact on firm innovation, which is robust when considering different windows for measuring CISO in TMT's turnover.

Post-Hoc Analyses: Impacts of CISO Educational Backgrounds

Educational background is a source of knowledge beyond work experience (Tesluk & Jacobs, 1998). Given that the CISOs in our sample had diverse educational backgrounds, often outside of security, we supplemented our main results with additional analysis that includes CISO educational backgrounds. We first collected data from LinkedIn for all CISOs in our sample. We manually coded each CISO's educational background (more details in Appendix E), which allowed us to identify four common educational backgrounds, i.e., business, IT, STEM, and legal studies or criminology. We included business and IT educational background because the digital upper echelons literature largely looks at the contribution of the business and IT knowledge of CIOs (e.g., Jones et al., 2020, Preston & Karahanna, 2009a, Preston & Karahanna, 2009b). We included a third dimension of educational background, i.e., STEM, because most CISOs obtain IT skills by pursuing engineering degrees (Karanja, 2017). Since some CISOs also report to the chief legal officer (Kappelman et al., 2020), we considered the impacts of CISOs with legal studies or criminology educational backgrounds.

Similar to our main hypothesis testing analysis, we replaced the binary code of the variable *CISOTMT* with a categorical variable, indicating whether the firm (1) had no CISO presence in TMT, (2) had a CISO in TMT with an educational background of interest, or (3) had a CISO in TMT with a different educational background. We used the presence of a CISO in TMT with a different educational background as the baseline in all models. The results are shown in the second table in Appendix E, with each column representing a different educational background of interest. We found that both coefficients on CISOs in TMT with business ($\beta = 0.121$, $p < 0.1$ in Column 1) and IT educational backgrounds ($\beta = 0.133$, $p < 0.1$ in Column 2) were positive and significant. The results indicate that firms with CISOs in TMT with a business or an IT educational background are more likely to increase firm innovation than CISOs with other educational backgrounds. However, CISOs in TMT with STEM ($\beta = 0.012$, p = n.s.) and legal studies or criminology ($\beta = -0.040$, p = n.s.) backgrounds had an insignificant influence on innovation compared with CISOs in TMT without those educational backgrounds. One possible reason is that CISOs in TMT with legal studies or criminology backgrounds and STEM backgrounds focus more on the prevention of crime and less on aligning information security with business.

Additional Robustness Checks Using Alternative Measures

To ensure the robustness of results concerning industry turbulence, we ran analyses using four- and five-digit NAICS codes to define industry boundaries. As shown in the first table in Appendix F, the interaction term between generalist CISOs in TMT and industry turbulence is significant and negative, consistent with our hypothesis testing results. Hence, the results regarding the moderating impacts of industry turbulence are robust, even with alternative definitions of industry boundaries. In addition, we used the sample's median value as the threshold categorizing specialist and generalist CISOs in TMT. As shown in second table in Appendix F, the results are consistent.

Discussion

Summary of Main Findings

This research examines the antecedents of CISO presence in TMT and its impact on firm innovation through a longitudinal analysis of S&P 1500 firms. Our results show that peer firms' CISO presence in TMT and their data breaches increase the focal firm's CISO presence in TMT. CISO presence in TMT increases firm innovation. However, appointing only a mid-level information security manager without a TMT designation does not affect firm innovation. Turnover of CISO in TMT also reduces firm innovation. Thus, the identified innovation effects can be isolated to CISO *presence* in the *TMT*. This finding is consistent with interviews with several CISOs. For example, the Mastercard[8] and Johnson & Johnson[9] CISOs expressed concern about the potential negative effects on innovation and business operations that can be introduced by information security policies and discussed how they ensure that their firms have the "right" level of risk. While companies with and without CISOs in TMT may have similar risks, CISOs in TMT can better allocate risks to align with business value-creating activities, such as innovation.

We also empirically identified the mechanisms that explain the positive effects of CISO presence in TMT on firm innovation. Specifically, the identified effects are driven by two mechanisms: (1) TMT CISO's better risk assessment communication with TMT

---

[8] Source: Ron Green - Mastercard: 'Ask the CISO. An Always On Environment Is Always Connected. Ron Green, EVP & CSO, Mastercard.' *CyberCrime Magazine.* https://soundcloud.com/cybercrimemagazine/ron-green-092719
[9] Source: Marene Allison - Johnson&Johnson: 'CISO 500 Interviews. Security In Healthcare. Marene Allison, CISO, Johnson & Johnson.' *CyberCrime Magzine.* https://soundcloud.com/cybercrimemagazine/ciso-500-marene-allison-vp-ciso-at-johnson-johnson

can inform other TMT about the security risk of innovation projects and (2) the development of a more secure environment fosters the innovation development process. However, the role of CISO presence in TMT in helping the firm adopt innovative IT products that improve access to external resources or knowledge has limited implications for explaining the impact of CISO presence in TMT on firm innovation.

Furthermore, we examine the heterogeneous effects of the presence of specialist and generalist CISOs in TMT. Our findings indicate that firms with specialist CISOs in TMT (i.e., those with richer prior work experience in the firm's focal industry) have more innovation than firms without CISOs in TMT. The positive effect of specialist CISOs in TMT on innovation is also significantly stronger than the effect of generalist CISOs in TMT (i.e., with more experience in industries other than that of the focal firm). This result is due to the uniqueness of the information security context, where "different firms in different industries have different threat profiles"[10]. Specialized CISOs' better understanding of industry-specific security risks allows them to apply security strategies without harming the company's innovation. Moreover, the relationship between generalist CISO presence in TMT and firm innovation depends on industry turbulence, i.e., the presence of a generalist CISO in TMT is positively associated with firm innovation in less turbulent industries.

Because information security is a relatively new profession (Zadelhoff, 2017) and CISOs may not have formal security training, we observe that CISOs come from different

---

[10] Source: Christopher Porter – Fannie Mae: 'Chris Porter Goes From The Cyber Trenches To Fortune 500 CISO' *CyberCrime Magzine.* https://cybersecurityventures.com/chris-porter-goes-from-the-cyber-trenches-to-fortune-500-ciso/

non-security educational backgrounds (i.e., most commonly from IT, business and law, or criminology) and accumulate industry experience. Therefore, we conducted additional empirical analyses to assess whether CISOs in TMT with different educational backgrounds influence firm innovation differently. We found that CISOs in TMT with formal education in IT or business have a greater positive impact on firm innovation than CISOs in TMT with other educational backgrounds. We did not find significant differences in innovation for firms with CISOs in TMT with legal, criminal justice, or STEM backgrounds. Taken together, our findings paint a clear picture of how appointing CISOs in TMT with different industry experience and educational backgrounds affects firm innovation.

Theoretical Implications

This research theoretically contributes to three streams of literature - information security, digital upper echelons, and TMT. First, our paper contributes to the information security literature by moving beyond the currently dominant view of the primary impact of CISO in TMT on firm security strategies and performance and highlighting the impact of CISO in TMT on business value creation. In arguing for the business value of CISO in TMT, we found a positive impact of CISO presence in TMT on firm innovation. Specifically, prior literature has focused on the impact of CISOs on information security, particularly with respect to the evolving security landscape (Maynard et al., 2018) and information security functions (Steinbart et al., 2018). In doing so, these studies implicitly assumed that information security is an IT function and did not focus on the impact of information security on business outcomes, such as innovation. Information security and business operations are interconnected and inseparable; therefore, a CISO's information security management responsibilities in TMT can change the business process, technology, and environment. Such changes, in turn, create opportunities for business value creation, such as innovation.

In addition, our findings offer implications for better evaluating and understanding the presence of CISOs in the TMT and information security investments in general. Previous literature has highlighted the challenges for CISOs to be legitimate as a TMT member, and accordingly suggested how a CISO can improve legitimacy judgments by other TMT members and the board of directors (e.g., Vance et al., 2022). In contrast to previous studies, we demonstrate the importance of the external industry environment in shaping a firm's decision to appoint a CISO to the TMT. Specifically, we find that industry peers' designation of a CISO in the TMT and security breaches provide institutional forces for the focal firm to move the CISO to the TMT. In doing so, we complement the prior inward-looking understanding of CISO legitimacy within a firm with an alternative view from external industry peers to explain CISO presence on the firm's TMT. In addition, metrics of information security leaders' in-role responsibilities, such as the nonoccurrence of information security incidents and deterrence of potential threats, are often evaluated unfavorably or inconsistently by board members (Doan, 2019) because a firm's board members often pay more attention to the business value generated from an executive's in-role responsibilities. In this research, we move beyond the security impact of CISOs in TMT and focus on the innovation impact to demonstrate another dimension of the value of CISOs in TMT within firms.

This research contributes to the literature on firm innovation from the perspective of digital upper echelons, i.e., technology-related TMT members, by examining the role of CISOs. Prior literature has demonstrated that digital upper echelons, such as CIOs, chief digital officers, and chief data officers, can improve innovation by directly leading innovation projects (e.g., Chau et al., 2020, Chen et al., 2021, Lee et al., 2014, Leidner et al., 2010, Li et al., 2021, Tumbas et al., 2018). Compared to these digital upper echelons, our theoretical premise is that although CISOs do not often directly initiate innovation, the influence of CISOs' in-role responsibilities on information security risk management could have spillover effects on firm innovation.

This research also contributes to TMT studies by adding insights into the background of the CISO in two important ways. First, we highlight the uniqueness of the CISO's knowledge accumulation characteristics compared to other TMT members examined in previous studies (e.g., Wang et al., 2015, Custódio et al., 2019). Specifically, unlike other executives with established career paths, CISOs are only now emerging as leaders in organizations and are in short supply. While CISOs hold knowledge-intensive jobs that require a deep understanding of the security and business domain to fulfill their responsibilities, we found that few of our CISOs had a formal educational background in security (i.e., 16 out of 418 CISOs). Prior literature has identified education and work experience as the two most important sources of knowledge for TMT members (Tesluk & Jacobs, 1998). Thus, understanding how accumulated knowledge from work experience is important for firms to appoint CISOs in TMT. Given the recent emergence of CISO presence in TMT, most CISOs' educational background is in a non-security degree and they accumulate experience in the industry. While work experience in diverse industries can bring new knowledge to drive innovation in firms (Custódio et al., 2019), CISOs with more experience in the same industry can better contribute to innovation due to the need for regulatory compliance, similar security risk profiles, and the importance of communication and coordination. Second, we demonstrate several unique contextual findings related to CISO educational background and highlight the benefits of appointing CISOs with IT or business backgrounds in TMT to facilitate business innovation. Overall, our findings provide a nuanced and contextual understanding of the importance of CISO educational background and industry experience in driving business innovation.

Practical Implications

Our findings offer a wealth of practical implications for firms that elevate CISOs to TMT and those that seek to appoint CISOs to TMT. Our results observe that a significant number of firms tend to follow industry best practice in hiring CISO in TMT. We encourage firms that have not yet included CISO in TMT to consistently follow the industry practice of CISO presence in TMT. In addition to paying attention to the CISO presence in TMT of peer firms, the firm should also track data breaches of peer firms. The firm may experience similar information security risks as peer firms, which will be of concern to investors. Appointing a CISO in TMT can send a positive signal to investors.

By establishing the positive impact of CISO presence in TMT on firm innovation, our results suggest that firms recognize the potential of CISOs in TMT to impact more than information security; indeed, their leadership of security initiatives and fulfillment of job responsibilities may have spillover effects on firm innovation. Practitioners can use our findings to better understand the value of CISO presence in TMT, i.e., preventing security incidents should not be the only outcome that firms can expect from CISOs.

Importantly, CISOs' security-enhancing activities are often aligned with business processes and can help create a better environment for cultivating innovation activities.

Our contextual findings regarding the heterogeneous innovation impacts of CISO presence in TMT with different backgrounds are relevant for firms evaluating CISO candidates in TMT. Our findings suggest that firms should select CISOs with more experience in the firm's focal industry to leverage their understanding of industry-specific regulations, business operations, and industry-specific information security risks. In contrast, findings on other TMT members in the innovation literature suggest that executives and other key stakeholders from other industries can provide additional perspectives and thus facilitate innovation. Our findings suggest that firms should select CISOs with more experience in other industries only if the firm operates in a less turbulent industry. Our findings also suggest that the CISOs who are best able to support innovation have a formal educational background in IT or business. Thus, we inform the applied understanding of the innovation impact of hiring CISOs with different educational backgrounds in TMT.

Our findings also suggest that firms should reconsider a commonly used remediation strategy, i.e., firing the CISO after a major information security incident. Although CISOs are responsible for information security management, firms need to consider the trade-off of firing a CISO in TMT due to a security breach, as it will significantly reduce firm innovation. While firing the CISO in TMT may have symbolic power, recent studies have shown that security incidents do not necessarily reduce firm revenues, and firms may even observe a significant increase in intangible reputational capital after a minor security incident (Makridis, 2021). Thus, while firing the CISO in the TMT sector after a security incident may be seen as a way to deflect responsibility for the breach, such actions may not effectively remediate the incident. Overall, we urge managers to consider the importance of retaining CISOs in TMT to support innovation.

Limitations and Future Research

We acknowledge the limitations of the study and discuss avenues for future research. First, our empirical analysis relies primarily on secondary data sources. We cannot fully control for the completeness of CISOs reported in the BoardEx database. Future work could go out into the field and directly observe how CISOs with heterogeneous backgrounds and industry experience affect firm innovation. Second, this research focuses only on the presence of CISOs in TMT and the industry and educational backgrounds of CISOs. Future research could extend our findings to examine the impact of different CISO governance strategies, such as CISO structural power, reporting structure, and incentives in the compensation structure. Third, this research focuses on CISOs in the TMT industry. Future research could examine how CISOs as middle managers in the firm influence performance and use the results to suggest how CISOs can be better positioned in the firm.

In addition, our research suggests several other directions for future research. First, future research could examine how CISO presence in TMT affects other firm performance measures. Because the security function is embedded in business processes and operations, CISO presence in TMT may influence various firm performances related to security risks, such as investment orientation and firm growth. Second, future research could examine the impact of the emerging digital upper echelon members on firms. Our research takes the CISO as an example of the rise of the digital upper echelon. As more digital upper echelons are appointed in TMT, it is important to understand their various influences on firm performance. Also, a deeper understanding of how the combinations of different digital upper echelons and their interactions with other digital and non-digital upper echelons influence firm performance could make a significant contribution. Third, taking advantage of the wave of emerging digital upper echelons, future research could compare the different impacts of digital and non-digital upper echelons on relevant firm performance, such as financial and operational performance.

Conclusion

Firms are appointing CISOs to cope with the growing demands of managing information security. In this research, we go beyond the security impact of CISOs to examine the antecedents of CISO presence in TMT and its impact on firm innovation. We find that industry peers' CISO presence in TMT and their data breaches motivate the focal firm to appoint a CISO in TMT. In addition to the overall positive impact of CISO presence in TMT on firm innovation, we show that CISOs in TMT with more work experience in the focal firm's industry have a greater impact on firm innovation, but other CISOs in TMT with more experience in different industries from the focal firm promote innovation only in less turbulent industries. Our results also demonstrate the benefits of CISOs in TMT with business or IT education in improving firm innovation. Overall, this research argues for the value of CISOs in TMT. In doing so, we contribute to the growing literature on information security, innovation, and TMT. Our findings also provide insights for firms interested in appointing CISOs in TMT that are aligned with their innovation goals.

CHAPTER 3

THE INFLUENCES OF EXECUTIVE COMPENSATION AND BOARD CYBERSECURITY INTENSITY ON SEC DATA BREACH NOTIFICATION TIMELINESS

Introduction

> *"Companies are getting hacked more frequently but aren't disclosing the incidents in their regulatory filings, a trend that worries investors ….The reason many data breaches aren't reported to the SEC … is that the damage isn't 'material,' meaning it isn't significant enough to influence an investor's decision to buy a company's stock ….To use the SEC's yardstick – whether a data breach is material – company executives have to exercise judgment, striking a delicate balance." (Shumsky, 2016), Wall Street Journal*

The United States (U.S.) Securities and Exchange Commission (SEC) has directed public firms to disclose material data breaches. Material refers to events or news that may reasonably be expected to affect a company's stock value (Rose, 2021). Public firms use 8-K reports to notify investors of a material event, and these reports are typically filed with the SEC within a few days after the event (Lerman & Livnat, 2010). Recent SEC cybersecurity guidance similarly advises firms to use 8-Ks for timely notification of material data breaches (SEC, 2018). The SEC's calls for timely notification of material breaches stem from two motivations. First, investors need information on material cybersecurity events to make informed decisions. Evidence suggests that the timing and content of disclosure of material events, such as data breaches and cybersecurity events, influence firm valuation (Gordon et al., 2010; Wang et al., 2013). Second, absent timely notification, the SEC worries that it becomes possible for insiders to take advantage of undisclosed breach information and reap unwarranted profits (Lin et al., 2020). For example, insiders could sell stock before the SEC is notified of a material breach.

Given its focus on investor protection, it is ironic that the SEC has left it to firms' executives to decide when to formally report material data breaches.[11] Evidence from 2005 to 2017 suggests that firms waited an average of nearly three weeks from discovering a data breach (as reported in another public source) to report it to the SEC in an 8-K filing (Kamiya et al., 2021). Such variance may result from contrasting opinions among executives on whether to file an 8-K after a material data breach based on what constitutes a material breach, the time required to remediate the breach before disclosure, or fear of negative market reaction. Explanations for variance are important because research shows that investors penalize firms for delayed disclosure (Ashraf et al., 2022). And for regulatory efforts that seek to specify the permissible time frame under which firms must disclose a material data breach, it is important to identify factors that might influence firms' adherence to such a mandate.

In this paper, we consider how IT and non-IT executives' compensation influences the timely reporting of material data breaches to the SEC (which we refer to as "SEC data breach notification"). On the one hand, IT executives' compensation structure typically rests on solving day-to-day IT-related issues necessary to support firm operations (Liu &

[11] This is true historically, and for the period of our study, although there is pending regulation that mandates a maximum four-day period from discovery of a material data breach to its disclosure to the SEC (via an 8-K filing) (SEC 2022). The SEC is expected to rule on this regulation in April 2023. Even if passed, firms will still have leeway in terms of how quickly they disclose a material data breach, because the determination of materiality lies with the firms. On this point, the SEC states "we expect registrants to be diligent in making a materiality determination in as prompt a manner as feasible" (SEC 2022).

Preston, 2021; Riemenschneider & Armstrong, 2021). By contrast, non-IT executives' compensation often hinges on longer-term outcomes, such as firm performance, reputation, and market valuation (Hambrick & Wowak, 2021; Wowak et al., 2017). We suspect that this contrast in focus of executive incentive schemes - of day-to-day operations versus longer-term outcomes – likely results in different timeliness in reporting material data breaches to the SEC. Hence, our first research question: *How does the compensation of IT executives and non-IT executives differentially influence the timeliness of a firm's SEC data breach notification?*

Corporate boards of directors often assist in their firms' cybersecurity decisions, including those involving public communications about data breaches(Aguilar, 2014; Cheng et al., 2021; Higgs et al., 2016). Boards of directors also play a role in firms' communications with the SEC (Goh, 2008). We, therefore, conjecture that the board's access to knowledge and direct experience with cybersecurity and data breaches, which we term "board cybersecurity intensity," influences their evaluation of executives' decisions to report material breaches to the SEC. Specifically, we posit that board cybersecurity intensity will moderate relationships between executive compensation and notification timeliness, thus leading to our second research question: *How does the firm's board cybersecurity intensity moderate the relationships between IT and non-IT executive compensation and timeliness of SEC data breach notification?*

To investigate these questions, we conducted a longitudinal analysis of U.S. public firms that experienced data breaches during 2008-2020. We find that greater IT executives' compensation positively relates to timelier SEC data breach notifications via 8-Ks, but greater non-IT executives' compensation has the opposite effect. We also show that board cybersecurity intensity weakens the positive relationship between IT executives' compensation and notification timeliness but amplifies the negative relationship between non-IT executives' compensation and notification timeliness. In other words, in both cases, board cybersecurity intensity 'slows down' the communication of material data breaches to the SEC.

This research advances cybersecurity disclosure literature by delineating how IT and non-IT executives' compensation and role-based priorities shape the reporting of material data breaches to the SEC. Additionally, our findings counter the reasonable view that the board's social ties to previously breached firms will result in more timely cybersecurity communications from the firm. We find the opposite and, in doing so, challenge the SEC's ambition of more timely material data breach notifications resulting from increased cybersecurity expertise on the board of directors. We later elaborate on the gamut of research, practice, and policy implications of our research.

Background on the SEC Data Breach Notification Decision

Firms are expected to demonstrate "good faith" when deciding whether to disclose material data breaches (SEC, 2018). As described in the opening excerpt, firms' decisions on this matter are complicated because the SEC offers limited guidance on what constitutes materiality. These decisions are further complicated by a complex regulatory landscape of federal, industry, and state data breach disclosure laws (Rose, 2021; Young, 2013) that afford executives leeway in how they publicly communicate about data breaches. As a result, some firms strategically time their data breach notifications to public sources (Amir et al., 2018; Foerderer & Schuetz, 2022). In a similar way, executives can make strategic decisions on when to notify the SEC of a material data breach.

While it is uncertain as to when firms should report material data breaches to SEC, doing so in a timely manner is important for several reasons. First, the SEC issues regulatory fines, which constitute negative market signals, to firms that fail to disclose material breaches promptly. For example, Yahoo was fined $35 million by the SEC for a delayed disclosure.[12] Given the loss of typically sensitive data and its potential impact on capital markets, the SEC also argues that delayed reporting of material data breaches has negative societal implications. As a result, the SEC has reached settlements with a growing number of firms on this matter.[13]

Second, the SEC has become more aggressive in encouraging firms to file timely cybersecurity disclosures. For example, the SEC recently contacted hundreds of firms thought victimized by the Solar Winds cyberattack, asking them to voluntarily report in SEC filings on any data breaches and related damages stemming from the cyberattack.[14] The SEC's communications and threat of regulatory penalty is positioned to motivate executives towards more timely notification since the fines and damage to firm reputations can be substantial.

Third, stock markets can punish firms that fail to report material data breaches. This is because when a data breach is disclosed in an SEC filing, it presumably has been

---

[12] https://www.washingtonpost.com/news/business/wp/2018/04/24/yahoo-fined-35-million-for-failing-to-disclose-cyber-breach/
[13] e.g., see: https://www.gibsondunn.com/sec-settlement-reflects-increasing-sec-focus-on-cyber-disclosures/
[14] https://www.reuters.com/technology/exclusive-wide-ranging-solarwinds-probe-sparks-fear-corporate-america-2021-09-10/

deemed *material* by firm executives, thus constituting a significant cybersecurity incident (perhaps more so than the typical data breach disclosed to other public sources). When a firm delays the reporting of a material breach, it may be inferred that executives are acting in their own best interests and not their stakeholders', thus resulting in further damage to firm valuation.

While the combination of market forces and SEC enforcement make it sensible for firms to report material data breaches to the SEC, there is substantial variance in the timing of reports. Given the ambiguity in both the definition of material breaches and current requirements for notification timeliness, we direct attention to three sets of firm decision-makers involved in reporting data breaches: IT executives, non-IT executives, and boards of directors. We seek to understand how the interplay of these decision-makers shape SEC data breach notification timeliness. Accordingly, we draw on agency theory to explain how executive compensation and the board, in its monitoring role, influence the speed of filing such SEC notifications via 8Ks.

Theoretical Foundation

Executive Compensation and Decision-Making for IT and Non-IT Executives

Agency theory suggests that compensation provides an incentive system that shapes executives' decisions and actions (Wowak et al., 2017). Specifically, to limit executives acting in a self-interested manner (i.e., agency problems), agency theory argues that principals (e.g., shareholders) use compensation to align agent interests with those of the firm (Eisenhardt, 1989; Ross, 1973). For example, stock options can be used to focus executives on firms' long-term, strategic investments (Sanders & Hambrick, 2007). When compensation aligns executive and shareholder interests, agency theory suggests that executives will make the best decisions to preserve or increase firm value, given their abilities and available opportunities. To ensure that alignment persists, boards of directors can provide oversight and monitor the actions of executives (Zajac & Westphal, 1994). Within organizations, agency theory acknowledges that executive roles can require different incentive systems to align their interests with those of shareholders and that specialized board knowledge may be needed to effectively monitor executive behavior (Wowak et al., 2017; Zajac & Westphal, 1994).

When comparing IT and non-IT executives, differences in role-based priorities can be attributed to responsibility assigned for operational performance and market performance. IT executives are incentivized to focus on efficient and effective day-to-day IT operations (Liu & Preston, 2021; Nash/KPMG, 2018; Riemenschneider & Armstrong, 2021). For example, many IT executives' compensation rewards promptly identifying and resolving cybersecurity incidents that disrupt IT operations (Ghule, 2020; Morgan, 2020). As a result, firms with a Chief Information Officer (CIO) on the top management team act more quickly to recover damages and losses from a data breach (Zafar et al., 2016). Given that IT executives are incentivized to solve IT-related issues promptly, they likely focus on quickly remediating the causes and implications of a material data breach, thereby making them more apt to support faster reporting of the incident to the SEC.

By contrast, non-IT executives focus on longer-term outcomes, such as firm performance, reputation, and market valuation, and thus would logically prefer to take time to understand all ramifications of a material breach before notifying the SEC. Since the Chief Executive Officer (CEO) and Chief Financial Officer (CFO) are responsible for filing the 8-K, they are likely to consider the reputational and market costs of notifications and support developing plans to take additional steps to shore up firm cybersecurity prior to notifying the SEC of a material data breach. By doing so, these non-IT executives take action to ensure that their firms' stock prices recover following a material data breach announcement, as well as to address investor concerns that future types of data breaches may undermine firm valuation. To this point, research shows that firms who report material IT control weaknesses in SEC filings subsequently upgrade their IT infrastructures, presumably to appease investor concerns about IT control deficiencies (Haislip et al., 2016). Such actions designed to address investor concerns and preserve market value require taking additional time, making non-IT-executives more apt to support slower reporting of a material data breach.

Clearly, SEC data breach notification decisions are complicated by executives' different role-based priorities. In the following section, we develop hypotheses on how compensation offered to IT and non-IT executives induces their role-based priorities that differentially affect the timeliness of SEC data breach notification and how the board's cybersecurity intensity impacts these relationships.

Hypotheses Development

Executive Compensation and SEC Data Breach Notification Timeliness

Executive compensation consists of a combination of base salary, bonuses, stock options, and other long-term incentives (Conyon, 2006; Harris & Bromiley, 2007); it is often tied to firm performance metrics, both short-term and long-term (Westphal & Zajac, 1994). Considering the role-based priorities of IT executives, which include quickly understanding the complexity of data breaches, coordinating recovery, fixing the root cause, and developing effective remediation strategies (Gwebu et al., 2018), their compensation should be at least somewhat tied to successfully addressing these issues.

Accordingly, we contend that greater IT executive compensation encourages timelier SEC data breach notification based on the following rationale. First, as IT executives see their compensation increase, they can be expected to assume more role-based responsibility with respect to their jobs and professional obligations. Since IT executives are often rewarded based on swift and legally sound responses to data breaches (Ghule, 2020; Morgan, 2020), they should be motivated to promptly resolve a data breach as their compensation increases. Indeed, IT executives' roles are less focused on longer-term firm performance, such as stock options and future dividends, which can be negatively affected by a breach disclosure, and more so on remediating immediate IT-related issues. Second, this motivational scheme should be amplified by IT executives' expertise. IT executives such as CIOs and Chief Information Security Officers (CISOs) would understand the nature of the breach related to their domain, and while likely aware of the broader impact on the organization, they should require less time than non-IT executives to understand remedies and implications of the breach for firm operations. Consequently, IT executives are positioned to support timely reporting of material data breaches. Third, while IT executives may assist in preparing an 8-K report, they do not have to sign their names to it, thus limiting their legal liability for such disclosures compared to non-IT executives (i.e., CEOs and CFOs).

IT executives' involvement in the SEC filing decision is supported by evidence that links increased IT expertise on the top management team to more accurate and timely filings of financial reports with the SEC (Haislip et al., 2020; Haislip & Richardson, 2018). Notably, this past work differs from ours in that executive compensation is not considered, nor are the SEC filings specific to material data breaches. In summary, because IT executives are incentivized toward prompt resolution of data breaches, possess the expertise needed to understand the implications of a material data breach, and have limited legal liability for an 8-K filing, we expect that higher compensation for this executive group will lead to more timely SEC data breach notification. Hence:

H1: Compensation for IT executives is positively related to SEC data breach notification timeliness.

In contrast to IT executives, we contend that greater non-IT executives' compensation encourages slower reporting of material data breaches. Non-IT executives' compensation hinges on long-term outcomes, such as firm performance, reputation, and market valuation. Indeed, a key facet of non-IT executives' current and future compensation rests on successfully managing relationships with the SEC in order to optimize the firm's market valuation. Doing so requires non-IT executives exercising due diligence in crafting and certifying the accuracy of reports to the SEC. It follows that non-IT executives would take extended time to completely understand the causes of a data breach, as well as its remedies and ramifications for firm valuation. Moreover, filing an 8-K for a material data breach can damage a firm's reputation and financial performance (Bolster et al., 2010), which are both important drivers of non-IT executive compensation (Milbourn, 2003). As evidence of such a negative performance impact, (Tosun, 2021) found that over the five years following a data breach announcement, firms were more likely to reduce dividend payments. For such reasons, non-IT executives are likely to require more time to think through the long-term strategic implications of how they report a material data breach notification (e.g., remedies and implications for future firm performance). Likewise, delaying a material data breach notification to the SEC gives investors time to 'digest' the news of the breach, assuming the breach has already been publicly disclosed via a non-SEC source (e.g., state laws or other regulations that require breach disclosures), thus potentially limiting the negative market impact of the SEC notification. Finally, unlike for IT executives, the SEC can hold non-IT executives personally liable for inaccurate 8-K notifications, which can result in missed incentives and even loss of employment for these individuals (Berard, 2018). In summary, since filing a material data breach notification with the SEC can negatively affect non-IT executives' compensation (through diminished firm performance, reputation, and market valuation) and may create personal legal liability, we expect that higher compensation for this executive group will lead to less timely notification. Hence:

H2: Compensation for non-IT executives is negatively related to SEC data breach notification timeliness.

Moderating Influence of Board of Directors' Cybersecurity Intensity

In considering the role of the board (and our board cybersecurity intensity concept in particular) in the SEC data breach notification decision, we draw on research that includes board monitoring in conjunction with executive compensation (Wowak et al., 2017) and firms' strategic cybersecurity decisions (Cheng et al., 2021; Higgs et al., 2016). Research indicates that both IT and non-IT executives' decisions are influenced by the board of directors (Devers et al., 2007; Wowak et al., 2017; Yayla & Hu, 2014) and that executives' responses to compensation are contingent on characteristics of the board (Devers et al., 2007). In a similar vein, we argue that the board's actual and access to cybersecurity experience will shape executives' understanding of the implications of data breach notification, thus altering the degree to which compensation drives timely notification decisions. Specifically, we argue that board cybersecurity intensity, as captured by board members' social ties to previously breached firms, should moderate the impact of IT and non-IT executives' compensation on the speed of material data breach notification.

A key function of the board is bridging information gaps for executives (Dass et al., 2014; Nicholson & Newton, 2010). Research shows that board members who utilize various informal networks to gain knowledge and experience (Burt, 1980, 1992; Dass et al., 2014; Homroy & Slechten, 2019) can assist in executive decision making. Similarly, we argue that socially connected board members, with their links to previously breached firms, have gained important knowledge and experience on how to communicate to stakeholders following a data breach and thus can advise executives on how to form SEC data breach notification strategies.

We posit that IT and non-IT executives will equally feel the influence of board monitoring on their role-based behavior, such that board cybersecurity intensity will alter compensation-induced role-based predictions and the speed of material data breach reporting specified in H1 and H2. We anticipate that boards will use their direct experience and ability to access information through social networks to advise firms on SEC requests for data breach notification. When a board possesses higher cybersecurity intensity, it will be better positioned to monitor and advise executives in making decisions about when to report and what to include in an SEC breach notification. However, because boards with greater cybersecurity intensity are more likely to demand more information to resolve information asymmetries on the causes and consequences of cybersecurity breaches, they will likely require more time to gather the information necessary to resolve gaps in their understanding and slow the reporting of the data breach to the SEC. Because boards with higher cybersecurity intensity will be more alert to information gaps, we anticipate fulfilling this monitoring obligation, gathering information required to close information asymmetries, and reviewing reports will consume substantial time and may slow notification to the SEC.

To the extent that executives perceive that boards are monitoring cybersecurity decisions and actions, they are likely to act in ways that align with what the board desires (Wowak et al., 2017). For IT executives, whose compensation encourages timelier SEC data breach notification, we predict this relationship will be dampened by greater board cybersecurity intensity (i.e., a 'slow down' effect). Conversely, for non-IT executives, whose compensation encourages less timely notification, we predict this relationship will be magnified (i.e., further 'slowed down') with increased board cybersecurity intensity. Hence:

H3: Board cybersecurity intensity moderates the positive relationship between IT executive compensation and SEC data breach notification timeliness, such that the relationship becomes less positive (increases the time to notification).

H4: Board cybersecurity intensity moderates the negative relationship between non-IT executive compensation and SEC data breach notification timeliness, such that the relationship becomes more negative (further increases the time to notification).

Method

Data

We collected data from multiple sources to test our hypotheses. The unit of analysis is firm-quarter due to our focus on notification timeliness and the subsequent need for 'timely' firm financial indicators in our analysis – most such indicators are updated quarterly. As well, because we focus on data breach notifications to the SEC, we restricted our sample to U.S. publicly traded firms that experienced a data breach. We obtained public data breach announcements from three sources: Privacy Rights Clearinghouse, Audit Analytics, and the VERIS Community Database. After merging the breach announcements in these sources and filtering out duplicate records, we had 769 unique firms that experienced data breaches (note that we include only the first breach for each firm in our sample). We then obtained the SEC data breach notifications for these firms in 8-Ks. From Audit Analytics, we obtained a listing of 8-Ks that were filed specifically for data breaches, and we used this as our initial sample of SEC data breach notifications. We found 65 such 8-Ks in the Audit Analytics data, which matched to the breached firms in our sample. For completeness, we also searched the Edgar database (sec.gov/edgar.shtml) for cybersecurity-related 8-Ks for the breached firms in our sample. To ensure the 8-Ks were cybersecurity-related, we used the keywords from D'Arcy & Basoglu (2022) (see Appendix G) for the searches. We then manually searched through these cybersecurity-related 8-Ks and retained only those that were initial data breach notifications that matched to a breached firm in our sample. The process resulted in 29 additional 8-Ks, for a total of 94 8-Ks (i.e., SEC data breach notifications).

We obtained executive compensation data from ExecuComp, which collects executives' compensation data directly from each firm's annual proxy statement. The number of reported executives in each firm in our sample ranges from five to nine.[15] We collected firms' financial performance data from Compustat. To measure board cybersecurity intensity, we collected firms' board members' individual social network data from BoardEx, which provides the time overlap among board members in the same affiliation (e.g., clubs, universities, firms, etc.).

We then merged these data from the different sources based on ticker, board member identifier, and time. We removed observations once the firm disclosed a data breach in the SEC 8-K filing or was delisted. We also removed observations with missing values. Our final sample includes 17,020 firm-quarter observations for 725 firms for the period 2008-2020.

Variable Definitions

Dependent variables

Not all firms in our sample issued an SEC data breach notification (via 8-K). Additionally, although a firm may not have issued a notification in a specific quarter *t*, it may have done so in subsequent quarters. We addressed this issue by fitting a survival analysis (as described below), which accounts for the different scenarios using two dependent variables. Specifically, the censor variable, $Disclosed_{it}$, is a binary variable denoting whether the firm *i* has an SEC data breach notification in quarter *t*. If the firm *i*

[15] For most firms, the ExecuComp database includes the top five paid executives, but for some firms, it includes up to nine. See https://wrds-www.wharton.upenn.edu/documents/1403/ExecuComp_part1.pptx.

has a notification in quarter *t*, the continuous variable $Days_{it}$ indicates the number of days between the date when the firm *i* issued the SEC data breach notification during quarter *t* and the date in which the breach was publicly announced via another source, such as the Privacy Rights Clearinghouse, Audit Analytics, or VERIS Community Database. By contrast, if the firm *i* did not have an SEC data breach notification in quarter *t*, the variable $Days_{it}$ refers to the number of days between the end of quarter *t* and the non-SEC data breach announcement date.

Independent variables

We used executive compensation data as reported in SEC proxy statements, which includes salary, bonuses, option awards, stock awards, non-equity incentives, pension value and non-qualified deferred compensation earnings, and other annual compensation. To distinguish IT from non-IT executives, we used keywords in Appendix H, which we derived by manually coding the job titles of sampled executives in S&P 1500 companies and extracting keywords related to executive-level technology positions. After the categorization, we measured *IT Compensation* as the average compensation of the firm *i*'s IT executives (e.g., CISO, CIO, Chief Technology Officer, etc.) in quarter *t*. Similarly, we measured *Non-IT Compensation* as the average compensation of firm *i*'s non-IT executives (e.g., CEO, CFO, Chief Operating Officer, etc.) in quarter *t*. Both measures were log-transformed because they had highly skewed distributions (i.e., we used log (1+x) to avoid taking log on zeros).

Moderator

We measured board cybersecurity intensity using the firm's board members' social ties to previously breached firms. Specifically, we calculated the variable *Board*

Cybersecurity Intensity as the total number of connections from firm *i*'s independent board members (i.e., those who are not affiliated with the focal firm) to board members in other firms who had experienced a data breach prior to the quarter *t*. These connections could be from the same firm they had worked, a university, a club, etc. We also log-transformed this variable due to its highly skewed distribution.

Control variables

We include control variables related to firm financial performance, executive and board characteristics, and data breach characteristics because these variables may influence the firm's likelihood of SEC data breach notification. First, financial performance may influence a firm's data breach disclosures to the SEC and other public sources through institutional resources and pressures, stock market dynamics, and a shift in the incentives to disclose. Consistent with prior data breach studies, we controlled for a wide range of such firm financial indicators: firm size, return on assets, Tobin's q, leverage, asset tangibility, market-to-book value of assets, market-to-book value of equity, capital expenditures, research and development investments, and earnings-to-price ratio. Second, because executive characteristics could influence both their compensation and the SEC data breach notification decision, we included executives' age and gender as control variables. Also, given that board dependence may influence both executives' compensation and disclosure decisions, we included the ratio of dependent board members (i.e., those who are affiliated with the firm) to the total number of board members. Third, we controlled for the severity of the breach being considered for SEC notification and the public attention the breach garnered. Following Haislip et al. (2021), the severity of a data breach is rated from 0 to 7 to indicate low to high severity of the breach. Following (D'Arcy & Basoglu, 2022) we measured public attention by abnormal changes in Google search volume (obtained via Google Trends) on the name of the breached firm. Specifically, we calculated the average search volume for the three days immediately following the public breach announcement minus the average search volume on the firm's name during the ninety days prior to the announcement. Finally, we included both year and industry fixed effects. Industry fixed effects are based on two-digit SIC codes for industry sectors.

Table 3.1 summarizes the definitions and descriptive statistics for all study variables and Appendix I presents their correlations.

Empirical Approach

Not all firms in our sample have an SEC data breach notification by the end of our observed period, but they may provide notification afterwards. By using the duration of survival and censoring of data, survival analysis can effectively account for this concern. Among the different survival models, the Cox proportional hazard model is widely used due to its ease of interpretation and independence between covariate coefficients and baseline hazard. Accordingly, we specify the following Cox proportional hazard model:

$$\lambda_i(t, x) = \lambda_0(t)\exp\,(\boldsymbol{X\beta}) \qquad (1)$$

where t refers to the survival time, λ_0 is the baseline hazard, $\lambda_i(t, x)$ is the hazard function influenced by the vector of covariates $\boldsymbol{X}$, and $\boldsymbol{\beta}$ represents the vector of coefficients.

Table 3.1. Descriptive Statistics of Compensation and Data Breach Disclosure Paper

Variables	Description	Mean	S.D.	Min	Max
Dependent Variable					
Disclosed	Whether firm i discloses data breach in SEC 8-K filing at time t	0.01	0.07	0	1.00
Independent Variables					
IT Compensation	Log (1+ IT executive compensation)	1.34	3.05	0.00	11.60
Non-IT Compensation	Log (1+ Non-IT executive compensation)	5.66	4.01	0.00	11.46
Moderator					
Board Cybersecurity Intensity	Number of board member connections with other breached firms divided by total number of connections	0.03	0.38	0.00	5.77
Control Variables					
Firm Size	Log (1+ total asset) of firm i at time t	9.13	2.23	0.08	15.20
ROA	Net income divided by total asset of firm i at time t	0.01	0.06	-2.66	1.77
Tobin's q	Market value divided by asset replacement cost of firm i at time t	2.05	2.32	0.42	148.88
Leverage	Long-term debt and debt in current liabilities divided by 1000 times of stockholders' equity of firm i at time t	1.20	135.11	-12846.64	1955.62
Asset Tangibility	Property, plant, and equipment – total (net) divided by total asset of firm i at time t	0.20	0.22	0.00	0.95
MBA	Market-to-book ratio of asset: market value of assets divided by the book value of assets of firm i at time t	2.31	16.01	-1915.55	253.64
MBE	Market-to-book ratio of equity: market value of equity divided by the book value of equity of firm i at time t	0.02	60.63	-6664.84	1215.14

Table 3.1. (continued)

Variables	Description	Mean	S.D.	Min	Max
R&D	Research and development expenditure divided by total assets of firm i at time t	0.01	0.02	0.00	0.45
EPR	Earnings-to-price ratio: earnings per share divided by closing stock price at year-end of firm i at time t	0.01	5.25	-246.58	445.94
CAPEX	Net capital expenditure to assets: (Capital Expenditure – Sale of Property, Plant and Equipment)/Assets of firm i at time t	0.01	0.03	-1.05	0.45
Age	Log (1+Average age of firm i's executives at time t)	4.01	0.06	3.67	4.33
Gender	Ratio of male executives in firm i at time t	0.88	0.12	0.00	1.00
Dependent Board Ratio	The ratio of dependent board member number to the total number of board members	0.046	0.124	0.000	1.000
Breach Severity	Severity of data breach	1.38	2.05	0.00	7.00
Breach Public Attention	Abnormal Internet search activity for the name of the breached firm *i*; average search volume for three days after breach announcement minus the average search volume for the prior ninety days	1.44	8.90	-23.10	72.74
Industry Type	2-digit SIC industry code			10	99

Note: Number of observations: 17020.

To test the first two hypotheses concerning the direct effects of IT and non-IT executives' compensation, we include the following independent variables and control variables in the vector $\boldsymbol{X}$. Specifically,

$$\boldsymbol{X\beta} = \beta_1 IT\ Compensation_{it} + \beta_2 Non\text{-}IT\ Compensation_{it} + \mathbb{X}\boldsymbol{\delta} + \epsilon_i \quad (2)$$

where $\mathbb{X}$ indicates the vector of all control variables, $\boldsymbol{\delta}$ is the vector of coefficients on control variables including the controls and moderator shown in Table 3.1, and ϵ_i refers to the error-term.

To examine the moderating effects of board cybersecurity intensity, we further add its interaction terms with IT and non-IT executives' compensation into Eq (2). Specifically,

$$\boldsymbol{X\beta} = \beta_1 IT\ Compensation_{it} + \beta_2 Non\text{-}IT\ Compensation_{it} + \beta_3 Board\ Cybersecurity\ Intensity_{it} + \beta_4 IT\ Compensation_{it} \times Board\ Cybersecurity\ Intensity_{it} + \beta_5 Non\text{-}IT\ Compensation_{it} * Board\ Cybersecurity\ Intensity_{it} + \mathbb{X}\boldsymbol{\delta} + \epsilon_i \quad (3)$$

Results

Results of Hypotheses Testing

Table 3.2 shows the results of the Cox proportional hazard model estimations. As shown in Model 1, the coefficient on *IT Compensation* is positive and significant (β = 0.121, $p < 0.05$), indicating that IT executives' compensation is positively associated with SEC data breach notification timeliness. Specifically, a one percent increase in IT executive compensation increases the speed of notification by 12.86% ($e^{0.121} * 100\% - 1$). Hence, H1 is supported. Conversely, results in Model 1 indicate a negative and significant coefficient on *Non-IT Compensation* (β = -0.138, $p < 0.05$), demonstrating that

Table 3.2. Survival Analysis of Main and Moderating Effects

Variables	Model 1	Model 2
IT Compensation	0.121**	0.121**
	(0.055)	(0.055)
Non-IT Compensation	-0.138**	-0.138**
	(0.055)	(0.055)
IT Compensation * Board		-0.123***
Cybersecurity Intensity		(0.037)
Non-IT Compensation * Board		-3.255***
Cybersecurity Intensity		(0.268)
Board Cybersecurity Intensity	-12.119***	18.573***
	(0.408)	(2.230)
Firm Size	0.171**	0.171**
	(0.085)	(0.085)
ROA	-0.365	-0.365
	(1.632)	(1.632)
Tobin's q	0.002	0.002
	(0.051)	(0.051)
Leverage	0.000	0.000
	(0.000)	(0.000)
Asset Tangibility	0.964	0.964
	(1.356)	(1.356)
MBA	0.008	0.008
	(0.017)	(0.017)
MBE	0.007	0.007
	(0.011)	(0.011)
R&D	-31.119*	-31.119*
	(18.456)	(18.456)
EPR	0.642***	0.642***
	(0.240)	(0.240)
CAPEX	-6.675	-6.675
	(6.432)	(6.432)
Age	0.106	0.106
	(2.918)	(2.918)
Gender	-2.273*	-2.273*
	(1.168)	(1.168)
Breach Severity	0.049	0.049
	(0.080)	(0.080)
Breach Public Attention	0.038**	0.038**
	(0.015)	(0.015)

Table 3.2. (continued)

Variables	Model 1	Model 2
Board Dependent Ratio	-36.882***	-37.881***
	(0.425)	(0.425)
N	16976	16976
Year Fixed Effect	Yes	Yes
Industry Fixed Effect	Yes	Yes
Wald χ^2	103825.816	116949.362

Notes: Significance levels: *p < 0.1, **p < 0.05, ***p < 0.01; Clustered standard errors are in parentheses.

non-IT executives' compensation decreases the timeliness of SEC data breach notification. Specifically, a one percent increase in non-IT executive compensation decreases the speed of notification by 12.89% ($1 - e^{-0.138} * 100\%$). Thus, H2 is supported.

As shown in Model 2 in Table 3.2, the coefficient for the interaction of IT executive compensation and board cybersecurity intensity is negative and significant (β = -0.123, $p < 0.01$), indicating that board cybersecurity intensity weakens the positive relationship between IT executives' compensation and SEC data breach notification timeliness. Thus, H3 is supported. Also, the coefficient for the interaction of non-IT executive compensation and board cybersecurity intensity is negative and significant (β = -3.255, $p < 0.01$), indicating that board cybersecurity intensity amplifies the negative relationship between IT executives' compensation and SEC data breach notification timeliness. Therefore, H4 is supported.

Addressing Endogeneity Concerns

Because survival analysis is a non-linear model, we cannot directly utilize the two-stage least-squares (2SLS) method to address endogeneity. Hence, we leverage the control function approach for this purpose (Tchetgen et al., 2015). This approach helps maintain the exogeneity of a treatment or intervention variable from unobservable confounding factors by conditioning the treatment variable through a two-stage estimation (Heckman & Robb Jr, 1985). Specifically, the control function approach disintegrates the correlation between our endogenous explanatory variables (i.e., IT and non-IT compensation) and unobservable variables impacting our outcome variables (i.e., SEC data breach notification) (Wooldridge, 2010). In the first stage of the control function approach, we estimate the residuals $\hat{\Delta}_{1i}$ and $\hat{\Delta}_{2i}$ from the following equations:

$$IT\,Compensation_i = z\tau_1 + w\delta_1 + \Delta_{1i}$$

$$Non\text{-}IT\,Compensation_i = z\tau_2 + w\delta_2 + \Delta_{2i}$$

where z includes seven variables for state living cost in the state where the firm is headquartered. These variables are each state's annual housing price index, annual housing price index changes, annual wage, quarterly all-transaction housing index, quarterly purchase-only housing index, and expanded data index with and without seasonal adjustment.[16] We choose these state-level living-cost variables because they are likely related to executive compensation, but no plausible reason exists to expect that they would be related to a firm's SEC data breach notification. Hence, the state living-cost variables satisfy the exclusion restrictions in the second step of the control function approach. Finally, w includes all control variables specified in Table 3.1.

[16] Annual housing index data: https://www.fhfa.gov/DataTools/Downloads/Pages/House-Price-Index-Datasets.aspx; Wage data: https://www.dol.gov/agencies/whd/state/minimum-wage/history

Table 3.3. Control Functions

Variables	Model 1	Model 2
IT Compensation	3.518*	3.492*
	(2.025)	(2.025)
Non-IT Compensation	-1.245**	-1.236**
	(0.616)	(0.616)
IT Compensation * Board		-0.108***
Cybersecurity Intensity		(0.039)
Non-IT Compensation * Board		-3.395***
Cybersecurity Intensity		(0.043)
Board Cybersecurity Intensity		17.775
		(.)
Firm Size	-0.064	-0.062
	(0.136)	(0.136)
ROA	-3.262	-3.235
	(3.223)	(3.223)
Tobin's q	0.045	0.045
	(0.036)	(0.036)
Leverage	0.001	0.001
	(0.000)	(0.000)
Asset Tangibility	1.610	1.598
	(1.107)	(1.107)
MBA	0.007	0.007
	(0.013)	(0.013)
MBE	0.003	0.003
	(0.003)	(0.003)
R&D	-75.878**	-75.402**
	(37.722)	(37.711)
EPR	0.406*	0.404*
	(0.217)	(0.216)
CAPEX	-6.196	-6.138
	(4.495)	(4.494)
Age	13.010	12.891
	(9.427)	(9.423)
Gender	-3.011***	-3.008***
	(1.094)	(1.089)
Breach Severity	0.168*	0.167*
	(0.091)	(0.091)
Breach Public Attention	0.078***	0.077***
	(0.029)	(0.029)

Table 3.3. (continued)

Variables	Model 1	Model 2
Board Dependent Ratio	-178.796	-178.775
	(.)	(.)
N	16976	16976
Year Fixed Effect	Yes	Yes

Notes: Significance levels: *p < 0.1, **p < 0.05, ***p < 0.01; Clustered standard errors are in parentheses. We did not include industry fixed effects because the model with industry fixed effects cannot estimate the standard errors of coefficients on main variables for hypothesis testing.

In the second stage of the control function approach, we include IT compensation, non-IT compensation, $\hat{\Delta}_1$, $\hat{\Delta}_2$, and w as independent variables in the Cox proportional hazard model. Our second-stage control-function results corroborate our main results, as shown in Table 3.3, thus helping to alleviate endogeneity concerns.

Mechanisms and Additional Robustness Checks

Compensation Incentives

An assumption made when applying agency theory in our hypotheses development is that total executive compensation is indicative of executive incentives. However, the total executive compensation includes both fixed and variable portions, which may differentially influence the notification behaviors of IT and non-IT executives. Thus, we ran additional analysis to account for this possibility, to ensure the robustness of our main analysis results based on the total compensation measure. Specifically, we used the ratio of incentive compensation (i.e., compensation excluding fixed income, or variable compensation) to the total compensation when measuring IT and non-IT executives' compensation. As shown in Table 3.4, the results are consistent with our hypothesis testing results.

Table 3.4. Results Using Compensation Incentive Ratio

Variables	Model 1	Model 2
IT Compensation	1.258**	1.258**
	(0.567)	(0.567)
Non-IT Compensation	-1.425**	-1.425**
	(0.619)	(0.619)
IT Compensation * Board		-1.345***
Cybersecurity Intensity		(0.442)
Non-IT Compensation * Board		-19.889***
Cybersecurity Intensity		(2.056)
Board Cybersecurity Intensity	-12.137***	5.991***
	(0.414)	(1.533)
Firm Size	0.168*	0.168*
	(0.087)	(0.087)
ROA	-0.350	-0.350
	(1.673)	(1.673)
Tobin's q	0.003	0.003
	(0.052)	(0.052)
Leverage	-0.000	-0.000
	(0.000)	(0.000)
Asset Tangibility	1.003	1.003
	(1.327)	(1.327)
MBA	0.008	0.008
	(0.017)	(0.017)
MBE	0.007	0.007
	(0.011)	(0.011)
R&D	-31.755*	-31.755*
	(18.817)	(18.817)
EPR	0.564**	0.564**
	(0.237)	(0.237)
CAPEX	-6.667	-6.667
	(6.451)	(6.451)
Age	-0.344	-0.344
	(2.730)	(2.730)
Gender	-2.190*	-2.190*
	(1.140)	(1.140)
Breach Severity	0.049	0.049
	(0.080)	(0.080)
Breach Public Attention	0.038**	0.038**
	(0.015)	(0.015)

Table 3.4. (continued)

Variables	Model 1	Model 2
Board Dependent Ratio	-36.893***	-37.891***
	(0.427)	(0.427)
N	16976	16976
Year Fixed Effect	Yes	Yes
Industry Fixed Effect	Yes	Yes
Wald χ^2	105364.809	120906.708

Notes: Significance levels: *p < 0.1, **p < 0.05, ***p < 0.01; Clustered standard errors are in parentheses.

Alternative Explanatory Variables

A related concern is that our results regarding IT and non-IT executive compensation could be sensitive to different forms of compensation. To address this concern, we conducted additional analyses using four alternate compensation measures obtained from ExecuComp which have been used in prior executive compensation studies (Kronlund & Sandy, 2014). The first is *Total Compensation*, which includes salary, bonuses, option grants, restricted stock grants, long-term incentive plan payouts, other annual compensation, and all other compensation. The second is *Realized Compensation*, which is the actual received value of compensation incentives at the time the compensation can be traded in (i.e., exercised). Both *Total Compensation* and *Realized Compensation* are calculated under the 1992 compensation reporting format. The third is *Compensation Fair Value*, which includes salary, bonus, grant date fair value of total stock and options, non-equity incentives, change in pension value and nonqualified deferred compensation earnings, and all other compensations. And finally, the fourth is *Compensation Exercise Value*, which includes salary, bonus, value of stock at time of vesting and value of options at time of exercise, non-equity incentives, and all other compensations. Both *Compensation Fair Value* and *Compensation Exercise Value* are calculated under the 2006 FAS 123 format. As shown in Table 3.5, the results using the alternative compensation measures continue to support our main results, indicating that our results are not sensitive to these alternate compensation structures.

Table 3.5. Survival Analysis of Moderating Effects with Alternative Compensation Measures

Variables	Model 1	Model 2	Model 3	Model 4
Alternative Compensation	*Total Compensation*		*Realized Compensation*	
IT Compensation	0.116**	0.116**	0.113**	0.113**
	(0.056)	(0.056)	(0.055)	(0.055)
Non-IT Compensation	-0.137**	-0.137**	-0.135**	-0.135**
	(0.056)	(0.056)	(0.054)	(0.054)
IT Compensation * Board Cybersecurity Intensity		-0.111***		-0.185***
		(0.037)		(0.030)
Non-IT Compensation * Board Cybersecurity Intensity		-3.376***		-3.084***
		(0.263)		(0.229)
Board Cybersecurity Intensity	-15.666	18.575***	-15.663	17.467***
	(.)	(2.129)	(.)	(1.889)
Firm Size	0.171**	0.171**	0.172**	0.172**
	(0.085)	(0.085)	(0.085)	(0.085)
ROA	-0.367	-0.367	-0.357	-0.357
	(1.630)	(1.630)	(1.630)	(1.630)
Tobin's q	0.002	0.002	0.003	0.003
	(0.051)	(0.051)	(0.051)	(0.051)
Leverage	0.000	0.000	0.000	0.000
	(0.000)	(0.000)	(0.000)	(0.000)
Asset Tangibility	0.963	0.963	0.948	0.948
	(1.350)	(1.350)	(1.349)	(1.349)
MBA	0.008	0.008	0.008	0.008
	(0.017)	(0.017)	(0.017)	(0.017)
MBE	0.007	0.007	0.007	0.007
	(0.011)	(0.011)	(0.011)	(0.011)
R&D	-31.016*	-31.016*	-31.056*	-31.056*
	(18.450)	(18.450)	(18.481)	(18.481)
EPR	0.641***	0.641***	0.639***	0.639***
	(0.239)	(0.239)	(0.240)	(0.240)

Table 3.5. (continued)

Variables	Model 1	Model 2	Model 3	Model 4
CAPEX	-6.626	-6.626	-6.666	-6.666
	(6.422)	(6.422)	(6.426)	(6.426)
Age	0.017	0.017	0.060	0.060
	(2.928)	(2.928)	(2.930)	(2.930)
Gender	-2.260*	-2.260*	-2.266*	-2.266*
	(1.162)	(1.162)	(1.158)	(1.158)
Breach Severity	0.048	0.048	0.049	0.049
	(0.080)	(0.080)	(0.080)	(0.080)
Breach Public Attention	0.038**	0.038**	0.038**	0.038**
	(0.015)	(0.015)	(0.015)	(0.015)
Board Dependent Ratio	-45.885	-40.884***	-45.872	-37.870***
	(.)	(0.424)	(.)	(0.425)
N	16976	16976	16976	16976
Year Fixed Effect	Yes	Yes	Yes	Yes
Industry Fixed Effect	Yes	Yes	Yes	Yes
Wald χ^2	4395.574	134780.237	4346.642	116900.147

Notes: Significance levels: *p < 0.1, **p < 0.05, ***p < 0.01; Clustered standard errors are in parentheses; Moderating effect of Current Compensation cannot be estimated due to collinearity.

Table 3.5. (continued)

Variables	Model 5	Model 6	Model 7	Model 8
Alternative Compensation	*Compensation Fair Value*		*Compensation Exercise Value*	
IT Compensation	0.116**	0.116**	0.119**	0.119**
	(0.056)	(0.056)	(0.056)	(0.056)
Non-IT Compensation	-0.137**	-0.137**	-0.139***	-0.139***
	(0.055)	(0.055)	(0.054)	(0.054)
IT Compensation * Board Cybersecurity Intensity		-0.103***		-0.230***
		(0.038)		(0.051)
Non-IT Compensation * Board Cybersecurity Intensity		-3.386***		-3.239***
		(0.268)		(0.032)
Board Cybersecurity Intensity	-14.245***	18.676***	-12.830***	16.417
	(0.418)	(2.174)	(0.424)	(.)
Firm Size	0.171**	0.171**	0.174**	0.174**
	(0.085)	(0.085)	(0.086)	(0.086)
ROA	-0.366	-0.366	-0.361	-0.361
	(1.630)	(1.630)	(1.622)	(1.622)
Tobin's q	0.002	0.002	0.004	0.004
	(0.051)	(0.051)	(0.051)	(0.051)
Leverage	0.000	0.000	0.000	0.000
	(0.000)	(0.000)	(0.000)	(0.000)
Asset Tangibility	0.965	0.965	0.950	0.950
	(1.349)	(1.349)	(1.345)	(1.345)
MBA	0.008	0.008	0.009	0.009
	(0.017)	(0.017)	(0.017)	(0.017)
MBE	0.007	0.007	0.007	0.007
	(0.011)	(0.011)	(0.011)	(0.011)
R&D	-31.033*	-31.033*	-31.168*	-31.168*
	(18.455)	(18.455)	(18.537)	(18.537)
EPR	0.641***	0.641***	0.641***	0.641***
	(0.239)	(0.239)	(0.241)	(0.241)
CAPEX	-6.633	-6.633	-6.672	-6.672
	(6.420)	(6.420)	(6.446)	(6.446)
Age	0.045	0.045	0.085	0.085
	(2.935)	(2.935)	(2.906)	(2.906)
Gender	-2.258*	-2.258*	-2.293**	-2.293**
	(1.163)	(1.163)	(1.164)	(1.164)
Breach Severity	0.049	0.049	0.050	0.050
	(0.080)	(0.080)	(0.080)	(0.080)
Breach Public Attention	0.038**	0.038**	0.038**	0.038**
	(0.015)	(0.015)	(0.015)	(0.015)

Table 3.5. (continued)

Variables	**Model 5**	**Model 6**	**Model 7**	**Model 8**
Board Dependent Ratio	-42.886***	-40.884***	-38.877***	-44.875***
	(0.424)	(0.424)	(0.429)	(0.429)
N	16976	16976	16976	16976
Year Fixed Effect	Yes	Yes	Yes	Yes
Industry Fixed Effect	Yes	Yes	Yes	Yes
Wald χ^2	162962.176	134345.933	111968.068	125844.276

Notes: Significance levels: *p < 0.1, **p < 0.05, ***p < 0.01; Clustered standard errors are in parentheses; Moderating effect of Current Compensation cannot be estimated due to collinearity.

Quarterly Fixed Effect

For our main analysis, we estimate a hazard model with year fixed effects to control for time-specific heterogeneity. However, year fixed effects cannot account for potential seasonal events or trends. To control for such potential seasonal influences, we include quarter fixed effects instead of year fixed effects in additional analyses. As shown in Table 3.6, the results are consistent with the main results, indicating that seasonality is not a major concern in our analyses. Of note, however, is that quarter dummies have strong collinearity with other variables in our models, and so we present the models with quarter fixed effects as a robustness check rather than include them in the main analysis.

Table 3.6. Survival Analysis of Main and Moderating Effects using Quarter Fixed Effect

Variables	Model 1	Model 2
IT Compensation	0.132**	0.132**
	(0.052)	(0.052)
Non-IT Compensation	-0.141***	-0.141***
	(0.050)	(0.050)
IT Compensation * Board Cybersecurity Intensity		-0.434***
		(0.075)
Non-IT Compensation * Board Cybersecurity Intensity		-4.455***
		(0.432)
Board Cybersecurity Intensity	-15.513	29.799***
	(.)	(3.704)
Firm Size	0.168**	0.168**
	(0.083)	(0.083)
ROA	-2.174	-2.174
	(2.054)	(2.054)
Tobin's q	0.018	0.018
	(0.079)	(0.079)
Leverage	0.000	0.000
	(0.000)	(0.000)
Asset Tangibility	0.836	0.836
	(1.396)	(1.396)
MBA	0.007	0.007
	(0.020)	(0.020)
MBE	0.009	0.009
	(0.013)	(0.013)
R&D	-33.312*	-33.312*
	(19.590)	(19.590)
EPR	1.531	1.531
	(0.996)	(0.996)
CAPEX	-8.345*	-8.345*
	(5.004)	(5.004)
Age	-0.227	-0.227
	(2.994)	(2.994)
Gender	-2.208*	-2.208*
	(1.224)	(1.224)
Breach Severity	0.047	0.047
	(0.074)	(0.074)
Breach Public Attention	0.036***	0.036***
	(0.013)	(0.013)

Table 3.6. (continued)

Variables	Model 1	Model 2
Board Dependent Ratio	-46.108	-38.095***
	(.)	(0.611)
N	16976	16976
Quarter Fixed Effect	Yes	Yes
Industry Fixed Effect	Yes	Yes
Wald χ^2	2412.540	159778.162

Notes: Significance levels: *p < 0.1, **p < 0.05, ***p < 0.01; Clustered standard errors are in parentheses.

Alternative Firm Decision Makers

In our theoretical development and empirical analyses, we assume that top IT and non-IT executives share involvement in the SEC data breach notification decision. One may argue, however, that certain powerful/influential executives disproportionally drive such decisions. To address this concern, we segmented top executives based on prior literature that treats CEO and/or CFO as the key decision-makers in SEC filing decisions (Friedman, 2014). Accordingly, in the first analysis, we ran a model with CEO compensation and other executives' (non-CEO) average compensation as the two independent variables. As shown in Table 3.7, neither variable is significant. In a second analysis, we ran a model with CEO compensation, CFO compensation, and all other executives' (non-CEO and non-CFO) average compensation as the three independent variables. As shown in Table 3.8, none of these variables is significant. This set of robustness checks help rule out alternative explanations based on the CEO and CFO being key SEC notification decision-makers for firms and provides additional support for our categorization of IT and non-IT executives as decision-makers for SEC data breach notifications.

Table 3.7. CEO and Non-CEO Compensation Impacts on Disclosure

Variables	Model 1	Model 2
CEO Compensation	0.033	0.033
	(0.124)	(0.124)
Non-CEO Compensation	-0.135	-0.135
	(0.142)	(0.142)
CEO Compensation * Board Cybersecurity Intensity		0.062
		(0.088)
Non-CEO Compensation * Board Cybersecurity Intensity		-0.152
		(0.105)
Board Cybersecurity Intensity	-13.391***	-11.280***
	(0.404)	(0.390)
Firm Size	0.179**	0.174**
	(0.084)	(0.084)
ROA	-0.375	-0.344
	(1.623)	(1.653)
Tobin’s q	0.002	0.001
	(0.049)	(0.050)
Leverage	0.000	0.000
	(0.000)	(0.000)
Asset Tangibility	0.958	0.952
	(1.341)	(1.330)
MBA	0.007	0.007
	(0.016)	(0.016)
MBE	0.005	0.005
	(0.011)	(0.011)
R&D	-29.262	-29.392
	(18.271)	(18.489)
EPR	0.595**	0.594**
	(0.234)	(0.232)
CAPEX	-6.090	-6.258
	(6.296)	(6.207)
Age	-0.966	-0.798
	(3.004)	(2.963)
Gender	-2.206*	-2.184*
	(1.141)	(1.132)
Breach Severity	0.042	0.045
	(0.081)	(0.081)
Breach Public Attention	0.038***	0.038***
	(0.015)	(0.015)

Table 3.7. (continued)

Variables	Model 1	Model 2
Board Dependent Ratio	-40.849***	-34.838***
	(0.412)	(0.418)
N	16976	16976
Year Fixed Effect	Yes	Yes
Industry Fixed Effect	Yes	Yes
Wald χ^2	204165.774	42483.529

Notes: Significance levels: *p < 0.1, **p < 0.05, ***p < 0.01; Clustered standard errors are in parentheses.

Discussion

Motivated by the SEC's increased attention to timely data breach notification, this research investigated whether IT and non-IT executives exerted a different effect on speed with which firms notify the SEC of material data breaches (via 8-K filings). We posited that the different role-based incentives found in executive compensation packages would result in IT executives supporting faster and non-IT executives supporting slower compensation. Because the SEC has pointed to board cybersecurity expertise as important to ensure timely data breach notifications (Hartmann & Carmenate, 2021), we considered whether board members' social connections to previously breached firms, which we refer to as board cybersecurity intensity, moderated the relationship between executive compensation and data breach notification timeliness. Based on analysis of a panel dataset covering the period 2008-2020, our empirical results supported our arguments regarding the different influences of IT and non-IT executive compensation on SEC notification timeliness and the role of board cybersecurity intensity in moderating these relationships.

Table 3.8. CEO, CFO, and Others' Compensation Impacts on Disclosure

Variables	Model 1	Model 2
CEO Compensation	-0.004	-0.004
	(0.096)	(0.096)
CFO Compensation	0.062	0.062
	(0.088)	(0.088)
Other Executives' Compensation	-0.152	-0.152
	(0.105)	(0.105)
CEO Compensation * Board		-0.305***
Cybersecurity Intensity		(0.018)
CFO Compensation * Board		2.895
Cybersecurity Intensity		(.)
Other Executives' Compensation *		-5.454
Board Cybersecurity Intensity		(.)
Board Cybersecurity Intensity	-11.280***	13.324
	(0.390)	(.)
Firm Size	0.174**	0.174**
	(0.084)	(0.084)
ROA	-0.344	-0.344
	(1.653)	(1.653)
Tobin's q	0.001	0.001
	(0.050)	(0.050)
Leverage	0.000	0.000
	(0.000)	(0.000)
Asset Tangibility	0.952	0.952
	(1.330)	(1.330)
MBA	0.007	0.007
	(0.016)	(0.016)
MBE	0.005	0.005
	(0.011)	(0.011)
R&D	-29.392	-29.392
	(18.489)	(18.489)
EPR	0.594**	0.594**
	(0.232)	(0.232)
CAPEX	-6.258	-6.258
	(6.207)	(6.207)
Age	-0.798	-0.798
	(2.963)	(2.963)
Gender	-2.184*	-2.184*
	(1.132)	(1.132)
Breach Severity	0.045	0.045
	(0.081)	(0.081)
Breach Public Attention	0.038***	0.038***
	(0.015)	(0.015)

Table 3.8. (continued)

Variables	Model 1	Model 2
Board Dependent Ratio	-34.838***	-44.836***
	(0.418)	(0.418)
N	16976	16976
Year Fixed Effect	Yes	Yes
Industry Fixed Effect	Yes	Yes
Wald χ^2	127664.021	74755.295

Notes: Significance levels: *p < 0.1, **p < 0.05, ***p < 0.01; Clustered standard errors are in parentheses.

We found executive compensation is associated with the speed of SEC data breach notification. For IT executives, their compensation is positively related to more prompt notification. We reason this is because IT executives' incentives likely underscore their role-based obligations to quickly resolve IT problems (e.g., quick resolution of cybersecurity incidents) and ensure systems are available to users (Hausken, 2007). In contrast, we found higher non-IT executive compensation is associated with increased time to SEC data breach notification. We reason this is because non-IT executives' compensation incentives likely encourage considering a broader set of concerns, which takes more time when making data breach notification decisions. Taken together, our analysis supports the argument that incentives for groups of executives results in different effects on the speed of data breach notifications.

We found that board cybersecurity intensity positively moderated (i.e., slowed down) the relationships between IT and non-IT executives' compensation and notification time. We reason this is because boards with access to more oversight and advisory experience will take more time to evaluate the nature and severity of the data breach resulting in less timely notification. Notably, this view is inconsistent with the logic underpinning the SEC's current guidance, which suggests that increasing the cybersecurity experience will result in faster reporting of material data breaches.

Taken together, our results show that executive compensation and board composition, specifically, the board's access to cybersecurity experience, need to be considered when seeking to explain the timing of SEC data breach notifications. To our knowledge, our work is the first to look specifically at data breach expertise of the board, as opposed to general IT expertise, and our domain-specific results diverge from past findings that general IT expertise helps to increase the speed of non-cybersecurity-related 8-K filings (Haislip et al., 2020). Where prior work implies that SEC suggestions to add cybersecurity expertise to boards will increase reporting, our results imply that boards will slow material data breach notification in 8-Ks, perhaps due to taking more time to demonstrate due diligence in investigating the cause and consequences of a breach.

Theoretical Contributions

This study contributes to theory and research on executive compensation and cybersecurity disclosures. First, we extend understanding of effects of agency incentives found in executive compensation to the cybersecurity context and provide evidence that compensation schemes of IT and non-IT executives influence firms' strategic IT-related decisions. Hence, our work suggests that future work on executive compensation, and more broadly those of managerial incentives, should consider the specific role-based incentives of the parties involved. Relatedly, our study suggests that viewing executive compensation without accounting for the unique executive role may overlook important contextual elements that shape firm decisions. By showing the differing influences of IT and non-IT executives' compensation, we provide an impetus for future theorizing about contextual differences in firms' strategic decisions.

Our findings on board cybersecurity intensity extend research on IT expertise at the board level. This literature generally finds that board IT expertise increases stock values and provides more efficient IT utilization and timely information flows to investors (Haislip et al., 2016; Haislip et al., 2020; Haislip et al., 2021; Higgs et al., 2016; Li et al., 2021). Our results suggest that board cybersecurity expertise slows the speed of SEC data breach notification because the board will take more time to gather and evaluate relevant information. Thus, rather than encouraging quick decisions, our findings support the notion that board cybersecurity intensity results in firms making more methodical data breach notification decisions in terms of communicating with the SEC. Notably, our work operationalizes board-level expertise differently than the literature on executives, boards, and IT decisions. Past work has primarily operationalized board IT expertise in terms of a board member's professional background or university training in IT (Li et al., 2021).

In contrast, our operationalization incorporates access to cybersecurity expertise through social connections of board members to other executives and managers who have experienced data breaches. In this manner, our operationalization captures a form of board interlock, in which board members engage in social learning through their interpersonal connections and shared experiences (Cheng et al., 2021). In future work, researchers can examine whether similar interlocks result in lower or higher quality strategic decisions about cybersecurity.

This study also extends recent literature that examines why firms are less timely with or underreport data breaches to public sources (Amir et al., 2018; Foerderer & Schuetz, 2022; Haislip et al., 2020). We go beyond studies that examine the initial breach notification to operationalize timely reporting as the time between a breach being reported in another public source and the time it is disclosed to the SEC as a material event. This unique conceptualization makes possible the time between when firms presumably become aware of a breach and their reporting it to the SEC, and by doing so, enables consideration of the influence of competing groups of executives and board monitoring on SEC data breach notification. Future research could leverage a similar approach to examine other strategic IT decisions, such as developing new technologies, investing in IT infrastructure, or outsourcing IT. For example, research could evaluate the length of time between initial announcements of IT initiatives and reporting to the SEC actual capital expenditures as a proxy for the quality and care of planning to support updating IT infrastructure or the developing new IT-enabled competencies.

Practical Implications

In terms of practical implications, our study provides evidence that heterogeneity in executive compensation effects timely SEC data breach notification. When responding to data breaches, executives should be aware that the composition of the executive team may impact the speed with which they communicate the incidents to the SEC, assuming they are deemed as material events. Firms may want to implement reporting structures that take into account the priorities and goals of executives (e.g., that include IT and non-IT executives) to ensure a balanced decision is made regarding material data breach notifications.

For boards of directors charged with cybersecurity oversight, our study provides insight into why they may receive conflicting messages about material breaches from executives. When considering information provided by executives, it suggests board members consider the source of information (IT executive vs. non-IT executive) and the nature of their compensation. Because disentangling conflicting messages may take time, corporate boards would be well-served to create defensible, transparent internal processes for how to evaluate breaches and clear criteria for when to notify the SEC. Many boards use similar methods (e.g., clearly defined clauses, controls, and processes) to manage financial regulatory reporting, so tying these methods to cybersecurity communications is likely legally feasible and may help to limit firm liability (Barth & Schipper, 2008; Srinivasan, 2005).

Our findings are relevant to regulators attempting to ensure timely material data breach notification. First, our results regarding the moderating effects of board cybersecurity intensity seem counter to the SEC's current emphasis on increasing board-level cybersecurity expertise. If timeliness is the metric regulators want to encourage, they need to be aware that more experienced boards are not necessarily faster but likely more apt to make a methodical assessment of the breach and its severity. Second, our results suggest that board members consider how executives' incentives influence the reporting of material data breaches. If the SEC enforces a minimum time for material data breach notification, as it is attempting to do (see footnote 1), board members may want to revisit the incentives offered to executives for timely reporting of material data breaches. Failure to do so could result in firms' failing to adhere to updated SEC guidelines or worse, undermine the quality of the assessment of whether a breach is material or not. Taken together, our results suggest that board of directors be aware of their impact, and their executive teams' impact, on timely reporting of data breach notification decisions.

Future Research Directions

This study provides several avenues for future research. First, our study focuses on executive compensation, a predominant influence on executives' behavior in the literature. However, other factors might influence firms' SEC data breach notification timeliness. Potential firm-level and executive-specific factors could include disagreement amongst different types of executives, prior firm experience with data breaches, and value alignment within executive teams. There is a need for research on these and other factors as they relate to material breach notifications and cybersecurity risk if we are to fully understand how executives shape firm cybersecurity risk and reporting.

An understanding of executives' ethical and risk orientations could further inform understanding of how executives shape SEC data breach notification timeliness. For instance, different executives may have different value systems and moral beliefs regarding transparency of their firms' cybersecurity issues, such as material data breaches. Different types of breaches (e.g., personal data compared to purely financial data) could also engender different views among executives about the materiality of the breach and whether its public disclosure is necessary from a moral/ethical perspective. Research that considers such aspects within the executive team and how they may influence notification timeliness would be valuable.

Beyond executives, researchers may wish to further explore the effects of the board of directors on cybersecurity issues. Our study found counterintuitive results when looking at the interlocking nature of the board in handling SEC data breach notifications. Future studies that capture varying cybersecurity expertise of board members and sources of interlock could lead to better-designed board governance of cybersecurity.

Finally, broadly speaking, our work suggests time as a variable of interest for cybersecurity research and firm strategies in this domain. Time is an important concept in the cybersecurity context because the study of data breaches can involve multiple stages (i.e., prevention, mitigation, remediation). For instance, understanding the alignment of executive compensation and board expertise for the stages of prevention, mitigation, and remediation of data breaches could prove interesting. Expertise in each area could differ, with technical expertise influencing prevention differently than it influences remediation, and so on. Thus, a more nuanced understanding of the data breach life cycle, such as the role of executive compensation and board expertise in each stage, could be insightful for theory and practice and could further inform our understanding of what drives timely data breach notifications to the SEC and other public sources.

Limitations

This study has limitations. First, it is limited to executive compensation's effect on SEC data breach notification. Our focus on compensation is driven by our interest in understanding how executives' role-based incentives in conjunction with board monitoring influence firm cybersecurity decisions, but other factors could also influence notification timeliness. Further, to instantiate timely notification, we focused on one form of cybersecurity communication – SEC data breach notifications in 8-Ks. We did so because 8-Ks are investors' first exposure to cybersecurity information in SEC filings and thus can be considered firms' most proactive communicative efforts about material data breaches in this context. Focusing on 8-Ks, therefore, allowed us to conceptualize the timely notification concept vis-à-vis previous public reporting of a data breach to another source. Yet, future work could examine less timely SEC filings that might include material data breach notifications, such as quarterly (10-Q) and annual (10-K) reports, to possibly extend the time period of what constitutes a timely SEC notification.

Conclusion

Against the backdrop of increased SEC scrutiny of material data breaches, this study sought to understand how executives and board shape the timing of reports of material data breaches to the SEC. We found evidence that IT and non-IT executives' compensation exert competing effects on SEC data breach notification timeliness, such that higher IT-executive compensation results in faster reporting and higher non-IT executive results in slower reporting. Further, we found that board cybersecurity intensity – that is, the board's social connections to previously breached firms - slows the effect of compensation on material data breach notification for both IT and non-IT executives. Our study sheds light on how executive incentives and board characteristics influence the timeliness of data breach notifications to regulators, and our results are informative to policymakers who are concerned with increasing the speed of firms' communications about material data breaches.

CHAPTER 4

TO WHOM SHOULD CDOS AND CISOS REPORT? MODERATING IMPACTS ON DIGITAL TRANSFORMATION AND SECURITY AWARENESS

Introduction

The fast-evolving digital technologies, such as cloud computing and artificial intelligence, are transforming how firms organize and operate (Chen & Srinivasan, 2023). Firms are increasingly undergoing a digital transformation process, in which they implement digital technologies to automate business processes and embedded digital technologies into their core business models (Gaskin et al., 2014; Tilson et al., 2010). The prevalence of digital transformation has been steadily extended to the non-IT firms (Bass, 2018). However, digital transformation comes with high risks (Tabrizi et al., 2019). Statistics shows that about $900 billion investments in digital transformation were wasted out of the total $1.3 trillion in 2018, and more than 70% of digital transformation initiatives failed to reach their goals.[17] Prior research and practitioner guidelines have attributed such failures to the people's lack of the right mindset to adapt and the misaligned organizational practices (Tabrizi et al., 2019), calling for the need of dedicated top executives and their collaboration with other executives in the firm. In this regard, firms are increasingly designating Chief Digital Officers (CDOs) to be in charge with managing the firm's digital transformation (Tumbas et al., 2018).

---

[17] Source: https://www.forbes.com/sites/forbestechcouncil/2018/03/13/why-digital-transformations-fail-closing-the-900-billion-hole-in-enterprise-strategy/?sh=7c25071b7b8b

The widespread digital transformation also triggered information security risks, as evidenced in the growing number of security breaches in the past decade (Kwon & Johnson, 2014). Consequently, firms need to be strategic and sensitive to the awareness of security threats and appropriate security countermeasures at the firm-level, which help them align security risks with returns on security investments (Li et al., 2023). A growing number of firms are also appointing Chief Information Security Officers (CISOs) to manage the firm's information security (Kappelman et al., 2019).

Although firms are appointing CDOs and CISOs in response to the emerging strategic visions—i.e., digital transformation and security awareness, respectively, it shows inconsistency regarding to whom CDOs and CISOs report. For example, 31% of firms have the CDO report to the CIO, while 65% of firms let them report to non-IT executives, such as CFOs and COOs.[18] In a survey of European organizations, 54.3% of firms having the CISO report to the CIO, while 42.6% of firms let their CISOs report to non-digital upper echelons such as CFOs and COOs. Among US organizations, 72.3% of CISOs report to the IT head, i.e., defined as the highest position among the digital upper echelons, which often is the CIO or CTO in a firm (Kappelman et al., 2019; Karanja, 2017). Given the inconsistent practices, it is crucial to examine the reporting structures of CDOs and CISOs to better inform senior managers on how to govern these emerging leadership roles in firms.

Informed by the evidence above and the social categorization lens (Quinn & Macrae, 2005), we compare two types of reporting structure: (1) *within-group* reporting

---

[18] https://www.ibm.com/downloads/cas/0OGWOGAW

structure, where the CDO or the CISO reports to the IT head, and (2) *across-group* reporting structure, where the CDO or the CISO reports to the non-IT head. Research has highlighted the importance of the fit between firm strategic vision and reporting structure in determining firm performance (e.g., Banker et al., 2011; Lee et al., 2015). Hence, we propose the following research questions: (1) *How does digital transformation and the CDO's reporting structure jointly influence firm performance?* (2) *How does security awareness and the CISO's reporting structure jointly influence firm performance?*

Given that the business value of IT is often realized at multiple levels, such as business processes, firm, and market, we consider both retrospective and prospective performance for firms (Kohli et al., 2012; Kini et al., 2005). Retrospective performance, such as operating income, pertains to a firm's historical, short-term performance. In contrast, prospective performance, such as market-to-book ratio of asset, focuses on the market's current anticipation of the firm's potential long-term performance and represent the firm's growth opportunities.

We examine our research questions using a longitudinal dataset comprised of the S&P 1500 firms. Our results demonstrate that digital transformation is positively associated with the firm's retrospective and prospective performance. Compare with the CDO reporting to the IT head, firms with CDOs reporting to non-IT heads will weaken the positive relationship between digital transformation and prospective performance. In addition, security awareness is negatively associated with the firm's retrospective performance, which will be weakened if the firm having its CISO reporting to non-IT heads. In summary, our results demonstrate the benefits of CDOs reporting to IT head and CISOs reporting to non-IT head.

Our research extends the IT leadership literature by focusing on the performance implications of reporting structure of CDOs and CISOs. We also contribute to the digital transformation and IT security literature by delineating how the impacts of digital transformation and security awareness on firm performance are contingent on emerging IT executives' reporting structure. Our findings provide suggestions to practitioners regarding how to align the reporting structure of CDOs and CISOs with the firm's strategic vision—i.e., digital transformation and security awareness.

Literature Review

The Rise of Digital Upper Echelons

Upper echelon theory argues that top management team (TMT) members make the firm act as they do; suggesting that the presence of TMT members and variance in their characteristics can impact firm performance (Hambrick & Mason, 1984). In this research, we focus on digital upper echelons, i.e., defined as TMT members with IT-related responsibilities as their primary role in the firm, and distinguish them from non-digital upper echelons who are not solely focused on technology-related responsibilities such as CEOs, Chief Financial Officers (CFOs) and Chief Operation Officers (COOs). CIOs and CTOs are well-established digital upper echelons who manage and oversee the internal IT functions and align them with the business (Carter et al., 2011).

Rapid and disruptive changes in the IT landscape and associated managerial concerns have triggered the emergence of new digital upper echelon positions. For example, the emerging demand for digitalization and the focus of the CIO on business-wide issues not tied to digitalization creates a need for a CDO in firms (Tumbas et al., 2018). Statistics shows that 152 firms on the S&P 500 list have designated CDOs

(Metzler et al., 2021). In addition, the rising information security risks motivate the firm to designate a CISO to manage information security threats and respond to security incidents (Kappelman et al., 2019). According to the IT trend survey statistics (Kappelman et al., 2019), nearly half (45.7%) of organizations have dedicated management positions related to cybersecurity.

Given the emergence of digital upper echelons, firms are taking different governance approaches to integrate them into the TMT, i.e., to whom they report. As elaborated in the Introduction section, a digital upper echelon may report to IT or non-IT heads. The two reporting structures suggest at least two different strategies for firms. For example, CISOs reporting to the IT head indicates that security is treated as an IT problem, while CISOs reporting to non-digital upper echelons indicates that security issues are considered more business oriented. Although we elaborated on the different reporting structures using CISO as an example, similar practices are commonly seen in other rising digital upper echelons (Lee et al., 2014). Hence, it is crucial to examine the impacts of reporting structures concerning the rising digital upper echelons. Therefore, this research takes an initial step to investigate the extent to which a firm's rising digital upper echelons report to the IT head (i.e., referred to as within-group reporting) as opposed to reporting to a non-IT head (i.e., defined as across-group reporting) affects firm performance.

Reporting Structure of Digital Upper Echelons

Perhaps because the digital echelon is just now emerging, the limited research on reporting structure has focused on comparing scenarios when the CIO reports to CEO or CFO (abbreviated as CIO-CEO and CIO-CFO reporting structure hereafter). This literature has emphasized the firm's strategic vision, including both the overall strategic positioning and IT strategies, as the driver of CIO reporting structure choices. Specifically, firms positioning as cost leadership are more likely to have a CIO-CFO reporting structure, while those with differentiation positioning are more likely to have a CIO-CEO reporting structure (Banker et al., 2011). Research also found some similar results when extrapolating the generic firm strategic positioning to IT strategic vision—i.e., firms viewing IT resources as differentiation, innovation, or growth strategies tend to have a CIO-CEO reporting structure. However, firms primarily leveraging IT resources in cost reduction (i.e., cost leadership) do not show more possibilities of having a CIO-CFO reporting structure (Karanja et al., 2021). Furthermore, the literature has related CIO reporting structure with a different categorization of firm IT strategic visions, i.e., viewing IT resources as "transform," "automate," and "informate" (Al-Taie et al., 2014). They found that the "transform" vision of IT makes CIO more likely to report to CEO than firms viewing IT as "automated," "informate-up," or "informate-down" roles.

The prior literature has also compared the performance implications of different CIO reporting structures. Studies have advocated the superior performance of the CIO-CEO reporting structure than the CIO-CFO reporting structure. For example, the CIO-CEO reporting structure has higher maturity of management for both benefit/value-enabled and operations/service-enabled IT risks than other reporting structures (Vincent et al., 2017). Research also found the advantage of the CIO-CEO reporting structure over other reporting structures after considering different situations and their combinations, such as firm size (large or small firm), industry type (automate, informate, or transform industry), IT investments (low versus high IT intensity), and IT orientation (IT spending as strategic investments versus operational efficiencies) (Aljazzaf et al., 2019). Along with this finding, several studies suggest advantages accrue to the CIO-CEO reporting structure. First, the power of IT increases as the CIO report to the CEO. In this case, IT is more likely to create business value for the firm (Karanja et al., 2021). Second, the visibility of CIOs changes as they report to the CEO. CIO reporting to CEO can have a better business mindset and understanding of IT-business alignment (Preston & Karahanna, 2009, Zafar et al., 2016).

However, this does not necessarily mean the CIO-CEO reporting structure will always produce the best outcomes. Banker et al. (2011) found that the impacts of the CIO reporting structure (i.e., CIO-CEO versus CIO-CFO) are contingent on the firm's strategic vision, i.e., cost leadership or differentiation. Specifically, the CIO-CFO reporting structure produces better performance for cost leadership firms than the CIO-CEO reporting structure, because CFO strives to reduce cost. In contrast, the CIO-CEO reporting structure is associated with better performance than the CIO-CFO reporting structure for differentiation firms.

Overall, the literature has demonstrated the importance of the CIO reporting structure and the value of examining its contingencies on firm strategic visions. It is important to move beyond the well-established digital upper echelons such as CIO or CTO, because the emerging digital upper echelon positions are expanding in TMT, and evidence suggests their reporting structure varies in practice (Kappelman et al., 2021, Karanja, 2017). However, the understanding and guidance on "to whom these emerging digital upper echelons should report" is scant in both academic literature and practice. More specifically, the emerging digital upper echelons create the dilemma regarding whether they should report to executives within or outside of IT group. In this emerging field, only one exceptional study (i.e., Steinburg et al., 2018) has examined CISO's reporting structure and found that CISO reporting to outside of IT function will have more effective information security performance regarding leading (fewer internal control weaknesses related to security) and lagging measures (more detected and stopped attacks). Extending the limited existing digital upper echelon reporting structure literature, this research examines the impacts of both CDOs' and CISOs' reporting structures on firm performance.

Social Categorization Processing

Social categorization indicates that in a group with diverse individuals, those with similar features are often treated as ingroup members, while others with dissimilar features as outgroup members. Previous social categorization literature suggests that individuals are purposefully or unintentionally involved in social categorization due to such motivations as active-encoding conditions (Quinn & Macrae, 2005). Literature from this perspective has conceptualized social categorization based on various features such as demographic features (e.g., race, gender, and culture) (Stangor et al., 1992) and goal-related features (e.g., education and function) (Maner et al., 2012).

Research has also evaluated the impacts of social categorization, focusing on individual and group performance. For example, individuals tend to allocate more memory to ingroup members (Rule et al., 2010) and would favor minimal ingroup members in their impressions, attitudes, and behaviors (Ratner et al., 2014). At the group level, studies found that the variation in group interaction raised by cultural decomposition may have an impact on group performance (Hopkins & Hopkins, 2002).

In another example, research suggests that the social categorization with more females at the manager level will benefit the firm. Still, more females in the workforce will negatively impact firm performance (Lyngsie & Foss, 2017).

Such fundamental social motives drive individuals to categorize others based on whether they display task-related features (Maner et al., 2012). Individual function serves as the task-relevant feature. As the TMT members are experts in various disciplines (Menz, 2012), implicit categorizations exist in the TMT. For this reason, digital upper echelons such as CIO, CDO, and CISO all have IT-related responsibilities and backgrounds, and thus tend to take each other as ingroup members. Accordingly, digital upper echelons are likely to consider other non-IT function executives, such as CFO, Chief Strategy Officer (CSO), COO, and Chief Marketing Officer (CMO), as outgroup members. The leader from the same functional group shares the same task vision with subordinates and can understand the needs of achievement and growth of similar background subordinates.

Hypothesis Development

Informed by the social categorization processing lens, we categorize digital upper echelons' reporting structure into within-group and across-group reporting structures. As elaborated in Figure 4.1, we define *within-group reporting structure* as the case when a digital upper echelon reports to IT head. In contrast, if a digital upper echelon reports to non-IT head, we define as *across-group reporting structure*.

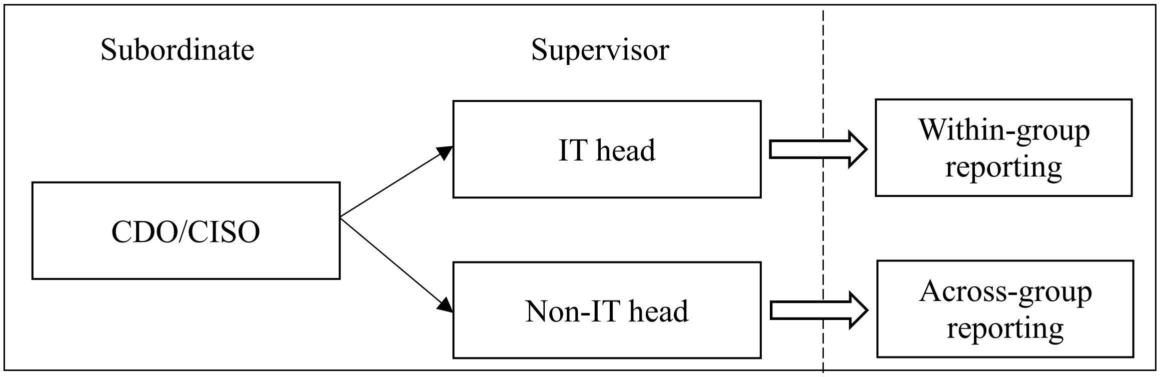

Figure 4.1. Reporting Structure Definition

Building on the prior literature's premise that executive reporting structure needs to be aligned with the firm's strategic visions and they often jointly influence firm performance (e.g., Banker et al., 2011; Lee et al., 2015), we theorize (1) how digital transformation influence firm performance and the moderating role of CDO reporting structures, and (2) how security awareness influence firm performance and the moderating role of CISO reporting structures.

We focus on both retrospective performance and prospective performance of firms, given their equal importance to inform senior executives (e.g., Kohli et al., 2012). Retrospective performance pertains to a firm's past performance, while prospective firm performance refers to the market's anticipation of the potential future performance of a firm within the current performance window (Kohli et al., 2012; Kini et al., 2005). In other words, retrospective performance reflects the firm's historical or short-term performance, while prospective performance focuses on the market's current anticipation of the firm's potential long-term performance. Digital transformation and security awareness can influence them differently based on their value generation and the market's perception of their value generation. Figure 4.2 summarizes the conceptual model.

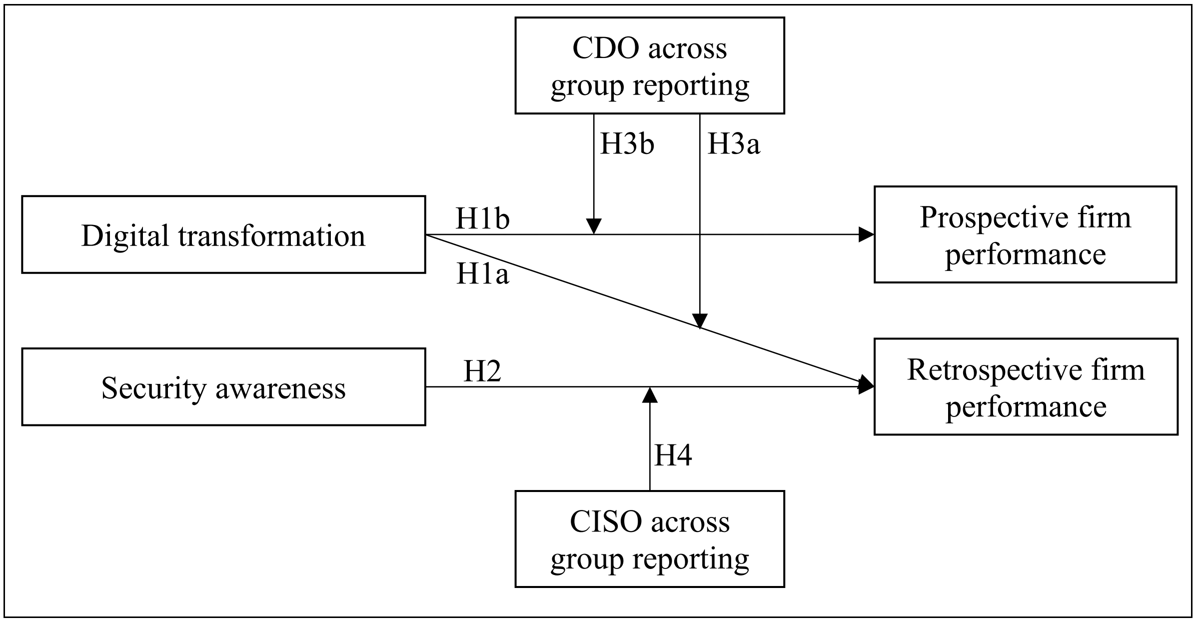

Figure 4.2. The Research Model of Reporting Structure

Effects of Digital Transformation on Firm Performance

Digital transformation can improve firm performance in the short run by reducing costs and enabling better decision-making. First, in the process of digital transformation, firms often implement digital technologies, such as enterprise resource planning, customer relationship management, or supply chain management systems. These digital technologies can help firms streamline and automate business processes (Fitzgerald et al., 2014; Hess et al., 2016). Consequently, the improved business process due to the digital technologies can reduce manual labor work, improve coordination among different departments, and inefficient practices. The reduced costs and improved operational efficiency can directly translate to the increased short-term operational performance (i.e., retrospective performance) in firms.

Second, digital transformation improves firms' decision-making by collecting and analyzing large amounts of data in diverse types (Li et al., 2021). For example, firms can use the data and available tools to assess their past performance more accurately, identify inefficiencies, and take corrective actions to improve productivity and reduce costs. Furthermore, firms can leverage real-time data analytics to make informed decisions, enhance data accuracy, and provide real-time visibility into key performance indicators. These digital transformation initiatives can optimize resource allocation and identify profitable opportunities to inform decision making, therefore increasing the firm's operational performance in the short run (i.e., retrospective performance). Hence, we hypothesize that:

Hypothesis 1a (H1a). Digital transformation is positively associated with the firm's retrospective performance.

Digital transformation also can enable the firms to survive in the hyper-turbulent environment and explore new business models to generate profit (Fitzgerald et al., 2014), which improves the firm's potential anticipation of long-term firm performance (i.e., prospective performance). First, digital transformation initiatives such as implementing e-commerce platforms, developing mobile applications, or utilizing artificial intelligence (AI) and machine learning (ML) enable firms to adapt to changing market dynamics (Witschel et al., 2019), therefore increasing their potentials for better long-term firm performance. For example, traditional brick-and-mortar retailers faced significant challenges due to the rise of e-commerce. These retailers implementing digital transformation would launch e-commerce platforms to cope with the changing business environments.

Second, digital transformation initiatives provide firms with the capabilities to explore new business models or revenue streams in the future (Fitzgerald et al., 2014). For example, after launching the e-commerce platform, firms can expand their customer reach and explore new business models such as omnichannel retailing (Gallino & Rooderkerk, 2020). This allowed them to tap into the online market. By integrating online and offline sales channels, these firms could provide seamless customer experiences and increase their potential for long-term performance. In addition, firms can leverage recommendation systems to provide personalized products, optimize pricing strategies, and deliver seamless customer experience.

In summary, the ability to adapt to changing market dynamics and to explore new business models results from the digital transformation can lead to a higher prospective performance for firms. Thus, we hypothesize that:

Hypothesis 1b (H1b). Digital transformation is positively associated with the firm's prospective performance.

Effects of Security Awareness on Firm Performance

Security awareness refers to the firm's overall sense of security threats and countermeasures (Li et al., 2023). Security awareness can influence the firm's retrospective performance by increasing security investments, slowing down business processes, and increasing potential remediation costs. First, as firms become more aware of security risks, they may invest more in security countermeasures such as firewalls, anti-virus software, and employee security training programs (Li et al., 2023; Kwon & Johnson 2014). While these investments can improve security protection capabilities and reduce security incident risks, they are also often costly, thus may decrease the firm's short-term retrospective performance.

Second, security countermeasures can sometimes be cumbersome and slow down business processes, decreasing efficiency and productivity (Tsai & Su, 2021). For example, implementing strict access controls may require employees to go through multiple authentication steps before accessing systems or data. This may require them to spend more time logging into systems or verifying their identities before accessing sensitive information, which often slow down their work and thus reduce their productivity. Hence, the increased security countermeasures resulted from the increased security awareness can decrease the retrospective firm performance.

Third, security awareness sometimes can be triggered by the firm's security incidents (Li et al., 2023), which can lead to lower retrospective firm performance. Security incidents can damage the firm's reputation and erode customer trust (Gwebu et al., 2018), decreasing sales and operating income. In addition, security awareness can increase the cost of remedying a security incident. To reduce the likelihood and impact of such incidents and minimize the negative effect, firms with security awareness can take proactive steps to improve security protection. The security strategic actions motivated by security awareness after the occurrence of security incidents can lead to decreased retrospective firm performance in the short run. Therefore, we hypothesize that:

Hypothesis 2 (H2). Security awareness is negatively associated with the firm's retrospective performance.

However, security awareness is not likely to influence the market anticipation towards the firm's long-term performance (i.e., prospective performance). Security awareness, in the long run, the investment of security tends to get steady, and will not cause additional negative impact on the firm's performance. In addition, in most cases, security is considered to protect the firm, similar as insurance, instead of a way to generate value for the firm. Therefore, the market will not have high expectations towards their long-term firm performance.

Moderating Effects of CDO Reporting Structure

Digital transformation often involves the implementation and integration of various digital technologies and systems across different departments within a firm (Hess et al., 2016). Reporting to the IT head ensures that the CDO has a direct line of communication with the IT-related departments that are responsible for managing and maintaining digital technologies. This allows for a more streamlined and efficient implementation of automation processes throughout the firm. However, if the CDO reports to a non-IT head, there may be a communication gap between the CDO and the IT departments. This can lead to delays or misunderstandings about the implementation and troubleshooting of digital systems. Hence, without the direct access to the IT head, the CDO may struggle to effectively coordinate and align automation efforts, potentially weakening the impact of digital transformation on process optimization and cost reduction.

Digital transformation often involves leveraging data analytics and real-time information to make informed business decisions (Li et al., 2021). Reporting to the IT head ensures that the CDO has a direct connection to the department responsible for managing data infrastructure, analytics tools, and data governance. This facilitates smoother data integration, analysis, and reporting processes. In contrast, if the CDO reports to a non-IT head, there might be limited influence or access to the necessary data and analytics resources. This can hinder the CDO's ability to collect and analyze data effectively, limiting the organization's capacity to make data-driven decisions. Without the necessary support and resources from the IT department, the positive impact of digital transformation on retrospective firm performance, in terms of accurate performance assessment, identifying inefficiencies, and seizing profitable opportunities, may be compromised. Hence, we hypothesize that

Hypothesis 3a (H3a). Compared with CDO reporting to IT heads, CDO reporting to non-IT heads will weaken the positive impact of digital transformation on the firm's retrospective performance.

When the CDO reports to the IT head, there is a stronger alignment between digital transformation initiatives and the firm's overall digital strategy. This alignment ensures that digital transformation efforts are integrated with the existing IT infrastructure, systems, and processes. It facilitates better coordination, collaboration, and support from the IT department, which is crucial for implementing complex technological solutions effectively. On the other hand, when the CDO reports to a non-IT head, there might be a misalignment of goals and priorities between the digital transformation initiatives and the digital strategy. This can result in difficulties in implementing and integrating new technologies, potentially hindering the company's ability to adapt to changing market dynamics.

Digital transformation is not solely a digital initiative, rather, it is a strategic business initiative that requires integration with the overall business strategy of the organization. When the CDO reports to the IT head, it becomes easier to align digital transformation efforts with the firm's strategic goals. The IT head can collaborate closely with other business leaders and ensure that digital initiatives are focused on achieving specific business outcomes. However, if the CDO reports to a non-IT head, there may be a lack of synergy between digital transformation initiatives and the broader business strategy. This can result in disjointed efforts, missed opportunities for innovation, and a limited ability to explore new business models effectively. Hence, we hypothesize that

Hypothesis 3b (H3b). Compared with CDO reporting to IT heads, CDO reporting to non-IT heads will weaken the positive impact of digital transformation on the firm's prospective performance.

Moderating Effects of CISO Reporting Structure

Compared with reporting to IT-head, CISO reporting to non-IT head can help optimize security investment outcomes and make more informed decisions regarding security countermeasures and remediation strategies. First, the CISO reporting to a non-IT head can better inform the non-IT head on the costs and benefits of security investments. Thus, the CISO reporting to a non-IT head is more likely to receive a "balanced" security budget that optimizes the returns on security investments and considers both security needs and the firm's overall performance goals. This balance can mitigate the negative impact of security awareness on retrospective firm performance.

Second, reporting to IT heads and non-IT heads can lead to different choices of security countermeasures that might influence the efficiency of business processes. When a CISO reports to an IT head, the focus may be primarily on ensuring that technical security countermeasures are in place with less consideration about the potential impacts on business operations. However, when the CISO reports to a non-IT head, the CISO can have a better understanding about the organization's business goals and objectives, which allows them to align security initiatives with long-term business strategies. From the non-IT head's perspective, they will balance security and operational needs. In this regard, they can provide insights and guidance on how to implement security countermeasures that have minimum disruptions to workflows and maintain productivity. This approach can help identify appropriate security measures that are effective, thereby weakening the negative impact of security awareness on retrospective firm performance.

Third, when the CISO reports to a non-IT head, the response to a security incident can be managed holistically—i.e., the remediation can consider legal, regulatory, public relations, and business continuity concerns beyond technical aspects, compared with reporting to IT head. This holistic remediation takes appropriate actions to restore trust, protect the brand reputation, and ensure business continuity, which minimizes the negative impact on the firm's retrospective performance. Therefore, we hypothesize that:

Hypothesis 4 (H4). Compared with CISO reporting to IT head, CISO reporting to non-IT head will weaken the negative impact of security awareness on the firm's retrospective performance.

Method

Data

We focused on S&P 1500 firms in our empirical analysis because these firms have relatively mature TMTs and S&P 1500 includes small, medium, and large companies. We compiled quarterly data of S&P 1500 firms during 2016-2020 from multiple sources. First, we collected each firm's reporting structure data from TheOfficialBoard, which contains detailed information of each individual executive's job title and supervisor (i.e., who they report to) for each firm. Second, we obtained earnings conference call through Eikon database to develop empirical measures of firm strategies, i.e., digital transformation and security awareness. Third, we gathered firms' executive-related data from ExecuComp and BoardEx. Fourth, we collected firm-level financial data and industry-level characteristics from Compustat and CRSP.

We merge the data from Compustat to TheOfficialBoard, earnings conference call, and CRSP data using the ticker as the unique identifier. Next, we merge the data with ExecuComp using gvkey as the unique identifier. Finally, we manually verified the accuracy of the matching—i.e., each identifier is corresponding to the same firm. We removed firms in the IT industry using the four-digital NAICS code that is consistent with Chung et al. (2019). Our final sample includes 12,979 observations after removing records with missing value.

Variable Definitions

Dependent Variables

We use industry adjusted operating income to measure the firm's retrospective performance (Kini et al., 2004; Kohli et al., 2012), denoted as *RetrospectivePerformance*. Specifically, we use log form of one plus operating income before the depreciation as the indicator of operating income. We measure the variable *ProspectivePerformance* using the industry adjusted market-to-book ratio of asset (Goyal et al., 2002; Kini et al., 2004) because it is often viewed as an indicator of a firm's potential for future growth, making it a useful tool for measuring prospective performance. We calculate the market-to-book ratio of assets as market value of assets divided by book value of assets. The market value of assets is calculated as the combined total of long-term debt, debt in current liabilities, and the product of the quarterly closing stock price and the common shares outstanding. The book value of assets is calculated as the sum of long-term debt, debt in current liabilities, and the total common/ordinary equity. We winsorized the measures at 99% to remove the outlier of the ratio measurement.

We normalized both the retrospective and prospective performance measures to the industry level (Kini et al., 2004; Chen & Srinivasan, 2023). Specifically, we calculate the industry-level median values for both market-to-book ratio and operating income within the focal firm's industry, identified by its five-digit primary NAICS code. We then compute industry adjusted market-to-book ratio and industry adjusted operating income by subtracting the industry median level of firm’s market-to-book ratio of assets and operating income from the focal firm’s corresponding market-to-book ratio of assets and operating income.

Independent Variables

We performed text mining on earnings conference call transcript to measure digital transformation and security awareness. The earnings conference call is a crucial communication channel for executives to discuss the company's financial performance with analysts and investors. During the call, executives can provide insights into the company's operations, financial position, and strategic direction, as well as answer questions from analysts and investors. The presentation provides a primary source of information without being interpreted by a third party, making them ideal for studying the beliefs and cognitive processes of top managers (Eklund & Mannor, 2021; Zhong et al., 2021).

We measure the variable *DigitalTransformation* using the total number of digital-related keywords, defined in Chen & Srinivasan (2023) and Metzler et al. (2021), that are appeared in the executive's presentation during the earnings conference call. Similarly, we measure *SecurityAwareness* using the total number of security-related keywords, defined in D'Arcy & Basoglu (2022), that are appeared in the executive's presentation during the earnings conference call. In consistent with our measures of dependent variables, we normalized digital transformation and security awareness measures to the industry median level. Specifically, we used the difference between the focal firm and the median value at focal firm's industry level, which is defined at level of five-digit primary NAICS code.

Moderators

We manually coded executive titles collected from TheOfficialBoard database to measure CDO and CISO reporting structure. First, we used a set of keywords to identify IT-related job titles.[19] This ends up with 6,213 unique job titles. Second, we manually coded each job title whether the responsibility is mainly IT related duties. We coded 331 job titles that have been used by multiple persons and firms by verifying whether the commonly accepted responsibility for these jobs is mainly IT related or not. For the rest 5,882 job titles which have been used for only one executive, we check each executive's responsibility through their LinkedIn page or description on company website to confirm whether their main responsibilities fall into any IT related duties.

[19] The keywords we used include: "cio," "cdo," "ciso," "data," "digit," "security," "info," "tech," "software," "system," "cloud," "app," "artificial," "internet," "mobil," "network," "wireless," "comput," "infrastructure," "architecture," "platform," "automation," "connectivity," "program."

Among the identified IT-related executives, we further manually coded whether each executive has security and digitalization related duties. We identified those IT-related executives with digitalization duties as CDOs, and those with security related responsibilities as CISOs. We define IT heads as the executives with IT-related responsibilities and directly report to CEO.

We coded two binary variables to measure the CDO's reporting structure in a firm. Specifically, *CDOWithinGroupReporting* equals one if the CDO reports to an IT head, and zero otherwise. *CDOAcrossGroupReporting* equals one if the CDO reports to a non-IT head, and zero otherwise. Similarly, we coded binary measures indicating CISO's reporting structure in a firm. *CISOWithinGroupReporting* equals one if the CISO reports to an IT head, and zero otherwise. *CISOAcrossGroupReporting* equals one if the CISO reports to a non-IT head, and zero otherwise.

Control Variables

We also control a set of variables that may affect a firm's performance and strategies. The first set of variables are related to firm characteristics. The natural logarithm of total assets controls *FirmSize*. We controlled *FirmAge* using the natural logarithm of one plus the number of years since the firm was listed. *BookLeverage* is the sum of long-term debt and debt in current liabilities scaled by total assets.

The second group of control variables we included are related to executives' characteristics. Specifically, we controlled the natural logarithm form of one plus total number of top management teams as *TotalTMT*. We included *AverageAge* as the natural logarithm form of one plus average ages of these TMT members. We controlled *FemaleRatio* measured by total number of females scaled by total number of TMT reporting compensation in proxy statement. We have also included CISO and CDO supervision related variables. Specifically, we include *AvgSub* as the natural logarithm form of one plus average number of subordinates in a group. In addition, we utilized two binary variables, *MoreCISOPeer* and *MoreCDOPeer*, which equal one if the CISO and CDO have more peers under the same supervisor than other groups within the firm, and zero otherwise, respectively. It accounts for if the CDO's and the CISO's supervisors are responsible for overseeing more subordinates than other supervisors within the firm.

We have also included the group of controls related to the firm's industry environments. Industry munificence controlled the opportunities of industry growth. Industry stability indicates the volatility of the industry. Following Keats & Hitt (1988), we measured industry instability and industry munificence by regressing industry average annual net income on year *t* using most recent five years data (*t* – *t*-4). We used

Table 4.1. Descriptive Statistics of Reporting Structure Paper

Variables	**Mean**	**S.D.**	**Min**	**Max**	**Data Source**
ProspectivePerformance	0.396	1.838	-2.741	11.246	Compustat
RetrospectivePerformance	-0.115	4.174	-8.898	9.469	Compustat
DigitalTransformation	0.051	0.262	-1.386	2.197	RefinitiveEikon
SecurityAwareness	0.061	0.344	-2.197	4.205	RefinitiveEikon
CDOWithinGroupReporting	0.015	0.120	0.000	1.000	TheOfficialBoard
CDOAcrossGroupReporting	0.030	0.169	0.000	1.000	TheOfficialBoard
CISOWithinGroupReporting	0.029	0.168	0.000	1.000	TheOfficialBoard
CISOAcrossGroupReporting	0.018	0.135	0.000	1.000	TheOfficialBoard
FirmSize	8.168	1.635	3.225	14.852	Compustat
FirmAge	3.234	0.636	0.000	4.094	CRSP
BookLeverage	0.306	0.258	0.000	3.945	Compustat
IndustryTurbulence	1.005	0.051	0.802	1.403	Compustat
IndustryGrowth	1.022	0.021	1.000	1.168	Compustat
MarketConcentration	0.081	0.086	0.010	0.595	Compustat
FemaleRatio	0.097	0.137	0.000	0.833	ExecuComp
AverageAge	3.230	1.590	0.000	4.251	ExecuComp

Table 4.1. (continued)

Variables	**Mean**	**S.D.**	**Min**	**Max**	**Data Source**
TotalTMT	0.696	1.408	0.000	4.787	ExecuComp
AvgSub	0.844	0.527	0.000	2.612	TheOfficialBoard
MoreCISOPeer	0.016	0.125	0.000	1.000	TheOfficialBoard
MoreCDOPeer	0.018	0.135	0.000	1.000	TheOfficialBoard

Note: Number of observations: 12979

exponential form of the standard errors and slope coefficient as *IndustryInstability* and *IndustryMunificence*, respectively. We also controlled *MarketConcentration*, which is measured using the Herfindahl–Hirschman Index—i.e., the sum of each firm's market share square scaled by focal industry total annual sales.

Table 4.1 summarizes the descriptive statistics and data sources for all variables. Appendix J presents the correlation matrix among all variables.

Empirical Approach

We apply ordinary least squares (OLS) as the baseline model in the empirical analysis. We also include firm and quarter-fixed effects in all models to account for firm-specific unobserved heterogeneity and time-invariant heterogeneity. We included time-variant controls to alleviate omitted variable bias. We used one quarter lagged dependent variable to help account for reverse causality. We estimated the following equations to test the main effects of digital transformation and security awareness.

$$\begin{bmatrix} RetrospecitvePerformance_{i,t+1} \\ ProspectivePerformance_{i,t+1} \end{bmatrix} = \alpha_i + \tau_t +$$

$$\beta_1 DigitalTransformation_{it} + \beta_2 SecurityAwareness_{it} + \sigma X_{it} + \epsilon_{it} \tag{1}$$

Where X_{it} indicates the vector of independent variables, moderators, and control variables and specified controls in Table 4.1. α_i accounts for the firm fixed effect, τ_t denotes the quarter fixed effect, and ϵ_{it} is the error term.

We added interactions terms to test the moderating effects of CISO and CDO reporting structures. Since our hypotheses compares CISO and CDO reporting to IT heads versus non-IT head, we leverage their reporting to IT head as the baseline, which allows us to directly examine the hypotheses using the significance of coefficients on the interaction between CISO and CDO reporting to non-IT and firm strategies, i.e., digital transformation and security awareness. Using the reporting to IT heads (i.e., within group reporting) as the baseline, we need to control for the scenario when firms are not having CISO or CDO reporting to either IT or non-IT heads, for which we coded as the variable *WithoutCISO* or *WithoutCDO*, respectively. Specifically, we estimate the following equations:

$$RetrospectivePerformance_{i,t+1} = \alpha_i + \tau_t + \beta_1 DigitalTransformation_{it} + \beta_2 SecurityAwareness_{it} + \beta_3 CDOAcrossGroupReporting_{it} * DigitalTransformation_{it} + \beta_4 CISOAcrossGroupReporting_{it} * SecurityAwareness_{it} + \beta_5 WithoutCDO_{it} * DigitalTransformation_{it} + \beta_6 WithoutCISO_{it} * SecurityAwareness_{it} + \sigma X_{it} + \epsilon_{it} \qquad (3)$$

$$ProspecitvePerformance_{i,t+1} = \alpha_i + \tau_t + \beta_1 DigitalTransformation_{it} + \beta_2 CDOAcrossGroupReporting_{it} * DigitalTransformation_{it} + \beta_3 WithoutCDO_{it} * DigitalTransformation_{it} + \beta_4 CDOAcrossGroupReporting_{it} + \beta_5 WithoutCDO_{it} + \sigma X_{it} + \epsilon_{it} \qquad (4)$$

where X_{it} indicates the vector of independent variables, moderators, and control variables and specified controls in Table 4.1. α_i accounts for the firm fixed effect, τ_t denotes the quarter fixed effect, and ϵ_{it} is the error term.

Results

Results of Hypothesis Testing

Table 4.2 shows hypothesis testing results. As shown in Column (1) in Table 4.2, the coefficient of *DigitalTransformation* is positive and significant ($\beta = 0.145$, $p < 0.1$). This implies that 1% increase in digital transformation compared with the industry norm leads to 14.5% more operating income. Hence, H1a is supported. Column (3) in Table 4.2 indicates that the coefficient of *DigitalTransformation* is significantly positive ($\beta = 0.095$, $p < 0.05$), indicates that 1% increase in digital transformation compared with the industry norm leads to 9.5% more market-to-book ratio of assets. This suggests that the market value of the company's assets has increased by 9.5% relative to their book value. In another word, investors have a more positive view of the firm's future prospects, which has driven up the market value of its assets. Therefore, H1b is supported.

The negatively significant coefficient of *SecurityAwareness* ($\beta = -0.235$, $p < 0.05$) in Column (1) indicates that 1% increase in security awareness reported in the earnings conference call compared with the industry norm leads to 23.5% less operating income. Hence, H2 is supported. Consistent with our theoretical argument, Column (3) shows an insignificant effect of security awareness on the firm's prospect performance ($\beta = -0.054$, p = n.s.).

As shown in Column (2) in Table 4.2, the coefficient of interaction between *CDOAcrossGroupReporting* and *DigitalTransformation* is negative but insignificant (β =

-0.759, p = n.s.), which implies that whether CDO reporting to IT head or non-IT head will not influence the impact of digital transformation strategy on retrospective firm performance. Therefore, H3a is not supported. Column (4) in Table 4.2 presents that the coefficient of interaction term between *CDOAcrossGroupReporting* and *DigitalTransformation* is significantly negative (β = -0.558, $p < 0.05$). This indicates that CDO reporting to non-IT head will weaken the positive impact of digital transformation on the firm's prospective performance, compared with CDO reporting to IT head. Hence,

Table 4.2. Results of IT Strategy and Reporting Structure Hypothesis Testing

Variables	**(1)**	**(2)**	**(3)**	**(4)**
	Retrospective Performance		**Prospective Performance**	
DigitalTransformation	**0.145***	0.549	**0.095****	0.459**
	(0.076)	(0.531)	**(0.047)**	(0.225)
SecurityAwareness	**-0.235****	-1.526**	-0.054	-0.054
	(0.107)	(0.760)	(0.049)	(0.049)
DigitalTransformation × CDOAcrossGroupReporting		**-0.759**		**-0.558****
		(0.596)		**(0.275)**
SecurityAwareness × CISOAcrossGroupReporting		**1.789****		
		(0.901)		
CDOAcrossGroupReporting	-0.151	-0.098	0.033	0.074
	(0.426)	(0.439)	(0.157)	(0.170)
CISOAcrossGroupReporting	1.029*	0.788	-0.053	-0.044
	(0.534)	(0.523)	(0.095)	(0.094)
Without CDO	-0.178	-0.157	0.133	0.148
	(0.429)	(0.432)	(0.103)	(0.104)
DigitalTransformation × WithoutCDO		-0.395		-0.359
		(0.533)		(0.221)
Without CISO	0.593*	0.488	0.027	0.031
	(0.352)	(0.338)	(0.078)	(0.079)
SecurityAwareness × WithoutCISO		1.330*		
		(0.769)		
FirmSize	1.063***	1.055***	-1.149***	-1.149***
	(0.203)	(0.202)	(0.218)	(0.218)
FirmAge	0.612	0.591	0.364	0.366
	(0.597)	(0.599)	(0.364)	(0.364)
BookLeverage	-0.389	-0.401	0.132	0.133
	(0.364)	(0.364)	(0.348)	(0.348)
IndustryTurbulence	1.042	1.083	-0.148	-0.143
	(1.116)	(1.112)	(0.479)	(0.480)
IndustryGrowth	-4.547	-4.523	1.004	1.006
	(5.753)	(5.738)	(0.922)	(0.923)
MarketConcentration	-1.949	-1.990	-0.111	-0.159
	(2.042)	(2.037)	(0.451)	(0.455)
FemaleRatio	0.102	0.103	0.013	0.008
	(0.317)	(0.318)	(0.193)	(0.192)
AverageAge	-0.017	-0.018	-0.002	-0.001
	(0.057)	(0.057)	(0.023)	(0.023)
TotalTMT	0.018	0.019	0.025	0.026
	(0.040)	(0.040)	(0.017)	(0.017)
AvgSub	-0.015	-0.010	0.025	0.025
	(0.074)	(0.074)	(0.045)	(0.045)

Table 4.2. (continued)

Variables	(1) Retrospective Performance	(2)	(3) Prospective Performance	(4)
MoreCISOPeer	-0.571	-0.426	-0.137	-0.136
	(0.477)	(0.470)	(0.097)	(0.096)
MoreCDOPeer	-0.563	-0.572	0.067	0.072
	(0.429)	(0.436)	(0.169)	(0.164)
Firm Fixed Effects	Yes	Yes	Yes	Yes
Quarter Fixed Effects	Yes	Yes	Yes	Yes
Number of Observations	11979	11979	11979	11979
R^2	0.022	0.025	0.07	0.07

Notes: Significance levels: $*p < 0.1$, $**p < 0.05$, $***p < 0.01$; Clustered standard errors are in parentheses.

H3b is supported. As shown in Column (2) in Table 4.2, The coefficient of the interaction between *CISOAcrossGroupReporting* and *SecurityAwareness* is positive and significant ($\beta = 1.789$, $p < 0.05$), indicating that the CISO reporting to non-IT head will mitigate the negative impact of security awareness on the retrospective firm performance. Hence, H4 is supported.

Robustness Checks

Industry-Specific Linear Time Trend

To account for unobserved confounding variables that changes between industries and overtime, we have included industry-specific linear time trend. Specifically, we included the interaction between each industry dummy variable (i.e., three-digit NAICS) and a continuous linear quarter time variable. As shown in Table 4.3, the results with industry linear time trends are consistent with our main results.

Table 4.3. Industry-Specific Linear Time Trend Model

Variables	(1)	(2)	(3)	(4)
	Retrospective Performance		Prospective Performance	
DigitalTransformation	**0.147****	0.541	**0.080***	0.458**
	(0.074)	(0.544)	**(0.045)**	(0.204)
SecurityAwareness	**-0.229****	-1.556**	-0.049	-0.049
	(0.100)	(0.762)	(0.048)	(0.048)
DigitalTransformation × *CDOAcrossGroupReporting*		**-0.598**		**-0.612****
		(0.601)		**(0.264)**
SecurityAwareness × *CISOAcrossGroupReporting*		**2.014****		
		(0.957)		
CDOAcrossGroupReporting	-0.201	-0.163	0.037	0.085
	(0.415)	(0.427)	(0.156)	(0.170)
CISOAcrossGroupReporting	1.068**	0.787*	-0.034	-0.024
	(0.498)	(0.471)	(0.095)	(0.094)
DigitalTransformation × *WithoutCDO*		-0.393		-0.371*
		(0.546)		(0.202)
SecurityAwareness × *WithoutCISO*		1.366*		
		(0.769)		
WithoutCDO	-0.230	-0.197	0.156	0.173*
	(0.414)	(0.418)	(0.102)	(0.104)
WithoutCISO	0.488	0.377	0.084	0.090
	(0.318)	(0.304)	(0.075)	(0.076)
FirmSize	1.085***	1.075***	-1.221***	-1.220***
	(0.205)	(0.205)	(0.215)	(0.215)
FirmAge	0.404	0.379	0.282	0.283
	(0.560)	(0.561)	(0.376)	(0.376)
BookLeverage	-0.622	-0.629*	0.111	0.114
	(0.380)	(0.380)	(0.348)	(0.348)
IndustryTurbulence	-0.151	-0.111	0.266	0.262
	(1.534)	(1.527)	(0.536)	(0.536)
IndustryGrowth	-6.401	-6.419	1.744*	1.736*
	(4.269)	(4.261)	(1.000)	(1.000)
MarketConcentration	-2.631	-2.685	0.169	0.114
	(1.653)	(1.643)	(0.429)	(0.433)
FemaleRatio	0.007	0.008	-0.041	-0.049
	(0.313)	(0.313)	(0.190)	(0.189)
AverageAge	-0.030	-0.031	0.002	0.003
	(0.030)	(0.030)	(0.014)	(0.014)
TotalTMT	0.002	0.002	0.032*	0.033*
	(0.037)	(0.037)	(0.017)	(0.018)
AvgSub	0.016	0.019	0.030	0.030
	(0.079)	(0.079)	(0.042)	(0.042)

Table 4.3. (continued)

Variables	(1) Retrospective Performance	(2)	(3) Prospective Performance	(4)
MoreCISOPeer	-0.772*	-0.612	-0.105	-0.105
	(0.465)	(0.450)	(0.090)	(0.089)
MoreCDOPeer	-0.734*	-0.742*	0.086	0.094
	(0.423)	(0.431)	(0.158)	(0.152)
Firm Fixed Effects	Yes	Yes	Yes	Yes
Quarter Fixed Effects	Yes	Yes	Yes	Yes
Industry Specific Linear Time	Yes	Yes	Yes	Yes
Number of Observations	11979	11979	11979	11979
R^2	0.053	0.053	0.089	0.089

Notes: Significance levels: *p < 0.1, **p < 0.05, ***p < 0.01; Clustered standard errors are in parentheses.

Alternative Definition for Non-IT Industry

In addition to our definition of IT industries using four-digit NAICS code (Chung et al., 2019), previous studies have used four-digit (Haislip et al., 2021) and three-digit (Kim et al., 2021) SIC code to define IT industries. Hence, we ran robustness checks by excluding additional firms that fall into the definition of four-digit and three-digit SIC code. In column (1)-(4) of Table 4.4, we present the results of excluding firms that are in the IT industry defined by four-digit NAICS code and four-digit SIC code. In column (5)-(8) of Table 4.4, we present the results of excluding firms that are in the IT industry defined by four-digit NAICS code, four-digit SIC code and three-digit SIC code. The results remain consistent with our hypothesis testing results.

Table 4.4. Alternative Definition for IT Industry

Variables	(1)	(2)	(3)	(4)
	Retrospective Performance		Prospective Performance	
DigitalTransformation	**0.139***	0.547	**0.095****	0.458**
	(0.076)	(0.532)	**(0.047)**	(0.225)
SecurityAwareness	**-0.236****	-1.529**	-0.054	-0.054
	(0.107)	(0.760)	(0.049)	(0.049)
DigitalTransformation ×		**-0.814**		**-0.549****
CDOAcrossGroupReporting		**(0.601)**		**(0.278)**
SecurityAwareness ×		**1.792****		
CISOAcrossGroupReporting		**(0.901)**		
CDOAcrossGroupReporting	-0.164	-0.107	0.036	0.075
	(0.428)	(0.440)	(0.158)	(0.171)
CISOAcrossGroupReporting	1.028*	0.788	-0.053	-0.044
	(0.534)	(0.523)	(0.095)	(0.094)
DigitalTransformation ×		-0.396		-0.358
WithoutCDO		(0.533)		(0.221)
SecurityAwareness ×		1.332*		
WithoutCISO		(0.769)		
WithoutCDO	-0.172	-0.151	0.137	0.152
	(0.430)	(0.433)	(0.103)	(0.105)
WithoutCISO	0.604*	0.501	0.031	0.035
	(0.353)	(0.338)	(0.078)	(0.079)
FirmSize	1.059***	1.052***	-1.156***	-1.156***
	(0.203)	(0.203)	(0.219)	(0.219)
FirmAge	0.604	0.583	0.354	0.356
	(0.599)	(0.600)	(0.365)	(0.365)
BookLeverage	-0.398	-0.411	0.129	0.130
	(0.364)	(0.364)	(0.348)	(0.348)
IndustryTurbulence	1.097	1.138	-0.118	-0.114
	(1.115)	(1.111)	(0.480)	(0.480)
IndustryGrowth	-4.435	-4.417	1.077	1.075
	(5.757)	(5.741)	(0.923)	(0.924)
MarketConcentration	-1.938	-1.980	-0.113	-0.160
	(2.043)	(2.038)	(0.453)	(0.457)
FemaleRatio	0.143	0.146	0.013	0.008
	(0.320)	(0.320)	(0.194)	(0.193)
AverageAge	-0.017	-0.018	-0.001	-0.001
	(0.057)	(0.058)	(0.023)	(0.023)
TotalTMT	0.024	0.025	0.027	0.028
	(0.040)	(0.040)	(0.017)	(0.017)
AvgSub	-0.017	-0.013	0.023	0.024
	(0.074)	(0.074)	(0.045)	(0.045)

Table 4.4 (continued)

Variables	(1)	(2)	(3)	(4)
	Retrospective Performance		Prospective Performance	
MoreCISOPeer	-0.564	-0.419	-0.136	-0.135
	(0.477)	(0.470)	(0.097)	(0.096)
MoreCDOPeer	-0.577	-0.588	0.074	0.078
	(0.432)	(0.439)	(0.169)	(0.165)
Firm Fixed Effects	Yes	Yes	Yes	Yes
Quarter Fixed Effects	Yes	Yes	Yes	Yes
Number of Observations	11940	11940	11940	11940
R^2	0.022	0.025	0.071	0.071

Notes: Significance levels: *p < 0.1, **p < 0.05, ***p < 0.01; Clustered standard errors are in parentheses.

Table 4.4 (continued)

Variables	(5)	(6)	(7)	(8)
	Retrospective Performance		Prospective Performance	
DigitalTransformation	**0.150***	0.550	**0.100****	0.461**
	(0.079)	(0.535)	**(0.048)**	(0.226)
SecurityAwareness	**-0.233****	-1.524**	-0.052	-0.052
	(0.108)	(0.762)	(0.050)	(0.050)
DigitalTransformation × *CDOAcrossGroupReporting*		**-0.818**		**-0.552****
		(0.603)		**(0.278)**
SecurityAwareness × *CISOAcrossGroupReporting*		**1.797****		
		(0.907)		
CDOAcrossGroupReporting	-0.163	-0.104	0.050	0.090
	(0.435)	(0.447)	(0.157)	(0.170)
CISOAcrossGroupReporting	1.046*	0.803	-0.061	-0.052
	(0.551)	(0.540)	(0.098)	(0.098)
DigitalTransformation × *WithoutCDO*		-0.387		-0.356
		(0.537)		(0.222)
SecurityAwareness × *WithoutCISO*		1.330*		
		(0.771)		
WithoutCDO	-0.160	-0.139	0.156	0.171
	(0.445)	(0.448)	(0.105)	(0.107)
WithoutCISO	0.613*	0.511	0.031	0.036
	(0.355)	(0.341)	(0.079)	(0.080)
FirmSize	1.011***	1.004***	-1.181***	-1.180***
	(0.200)	(0.200)	(0.222)	(0.222)
FirmAge	0.648	0.626	0.297	0.299
	(0.620)	(0.622)	(0.378)	(0.378)

Table 4.4 (continued)

Variables	(5)	(6)	(7)	(8)
	Retrospective Performance		**Prospective Performance**	
BookLeverage	-0.411	-0.423	0.124	0.125
	(0.364)	(0.364)	(0.349)	(0.349)
IndustryTurbulence	1.045	1.084	-0.146	-0.141
	(1.132)	(1.128)	(0.482)	(0.482)
IndustryGrowth	-4.354	-4.328	1.109	1.106
	(5.877)	(5.862)	(0.937)	(0.937)
MarketConcentration	-1.918	-1.956	-0.090	-0.137
	(2.087)	(2.082)	(0.458)	(0.462)
FemaleRatio	0.152	0.155	0.006	0.002
	(0.322)	(0.322)	(0.197)	(0.196)
AverageAge	-0.038	-0.039	-0.006	-0.006
	(0.054)	(0.055)	(0.023)	(0.023)
TotalTMT	0.028	0.029	0.028	0.028
	(0.042)	(0.042)	(0.017)	(0.017)
AvgSub	-0.023	-0.018	0.023	0.024
	(0.074)	(0.074)	(0.045)	(0.045)
MoreCISOPeer	-0.569	-0.422	-0.139	-0.138
	(0.489)	(0.482)	(0.099)	(0.099)
MoreCDOPeer	-0.575	-0.585	0.081	0.085
	(0.434)	(0.441)	(0.170)	(0.165)
Firm Fixed Effects	Yes	Yes	Yes	Yes
Quarter Fixed Effects	Yes	Yes	Yes	Yes
Number of Observations	11751	11751	11751	11751
R^2	0.021	0.024	0.072	0.073

Notes: Significance levels: **p* < 0.1, ***p* < 0.05, ****p* < 0.01; Clustered standard errors are in parentheses.

Falsification Test

As we focus on non-IT industries, it remains unclear whether the impacts we found are specific to the non-IT industry. Therefore, we ran a falsification test using the IT industries. The results, as shown in Table 4.5, indicate that the identified impacts in non-IT industries are not significant in IT industries. Hence, our theoretical development and findings are specific to firms in non-IT industries.

Table 4.5. Falsification Test - Impacts in IT Industry

Variables	**(1)**	**(2)**	**(3)**	**(4)**
	Retrospective Performance		**Prospective Performance**	
DigitalTransformation	0.096	-0.656	-0.058	-0.524
	(0.084)	(1.081)	(0.081)	(0.344)
SecurityAwareness	-0.123	-0.602	-0.063	-0.061
	(0.096)	(1.131)	(0.062)	(0.062)
DigitalTransformation ×		0.185		0.129
CDOAcrossGroupReporting		(1.220)		(0.812)
SecurityAwareness ×		0.752		
CISOAcrossGroupReporting		(1.136)		
CDOAcrossGroupReporting	-0.539	-0.168	-0.160	0.065
	(0.521)	(0.484)	(0.489)	(0.650)
CISOAcrossGroupReporting	1.114*	0.906	0.281	0.293
	(0.654)	(0.777)	(0.522)	(0.524)
DigitalTransformation ×		0.777		0.480
WithoutCDO		(1.088)		(0.341)
SecurityAwareness ×		0.499		
WithoutCISO		(1.137)		
WithoutCDO	0.131	0.023	0.285	0.214
	(0.621)	(0.592)	(0.441)	(0.391)
WithoutCISO	-0.606*	-0.727**	-0.280	-0.274
	(0.356)	(0.349)	(0.306)	(0.305)
FirmSize	1.651***	1.640***	-0.410	-0.417
	(0.320)	(0.320)	(0.362)	(0.365)
FirmAge	0.502	0.533	0.719	0.739
	(1.345)	(1.337)	(1.132)	(1.129)
BookLeverage	-2.350**	-2.402**	-1.885*	-1.900*
	(0.963)	(0.958)	(1.119)	(1.110)
IndustryTurbulence	-10.095**	-9.711**	-5.329	-5.139
	(4.560)	(4.615)	(5.112)	(5.176)
IndustryGrowth	-10.910	-11.034	-2.781	-2.894
	(11.983)	(12.206)	(12.928)	(12.922)
MarketConcentration	-12.505	-12.310	9.603	9.447
	(13.296)	(12.985)	(15.316)	(15.203)
FemaleRatio	0.122	0.101	0.633	0.618
	(0.752)	(0.742)	(0.803)	(0.793)
AverageAge	0.002	0.001	-0.203**	-0.203**
	(0.059)	(0.059)	(0.095)	(0.095)
TotalTMT	-0.015	-0.015	-0.028	-0.029
	(0.049)	(0.048)	(0.044)	(0.044)
AvgSub	-0.232*	-0.239*	0.063	0.059
	(0.139)	(0.139)	(0.142)	(0.143)

Table 4.5. (continued)

Variables	(1)	(2)	(3)	(4)
	Retrospective Performance		Prospective Performance	
MoreCISOPeer	-1.871*	-1.859	-0.779	-0.771
	(1.020)	(1.141)	(0.514)	(0.517)
MoreCDOPeer	0.303	0.177	0.402	0.325
	(0.474)	(0.487)	(0.436)	(0.357)
Firm Fixed Effects	Yes	Yes	Yes	Yes
Quarter Fixed Effects	Yes	Yes	Yes	Yes
Number of Observations	3188	3188	3188	3188
R^2	0.073	0.075	0.060	0.061

Notes: Significance levels: $^*p < 0.1$, $^{**}p < 0.05$, $^{***}p < 0.01$; Clustered standard errors are in parentheses.

Discussion

Against a backdrop of expanding top-level technology managers, this research provides timely insights into the governance of emerging digital upper echelons (i.e., CDOs and CISOs) and how it alters the performance implications of firm strategic visions, i.e., digital transformation and security awareness. Our robust longitudinal empirical analysis demonstrates that CDOs reporting to non-IT heads (i.e., cross-group reporting structure) weakens the positive associative between digital transformation and the firm's prospective performance, compared with CDOs reporting to IT heads (i.e., within-group reporting structure). We also found that CISOs reporting to non-IT heads (i.e., cross-group reporting structure) weakens the negative associative between security awareness and the firm's retrospective performance, compared with CISOs reporting to IT heads (i.e., within-group reporting structure). Overall, our results demonstrate the advantages of CDOs' within-group reporting structure (i.e., reporting to IT heads) and CISOs' across-group reporting structure (i.e., reporting to non-IT heads) to better align with the firm's strategic visions.

Theoretical Implications

This research adds to digital upper echelon literature by examining reporting structure of emerging digital upper echelons. Previous literature focuses on the performance of the CIO reporting structure (i.e., CIO reporting to CEO versus CFO) and its contingent impacts on the firm's strategic vision (e.g., Banker et al., 2011). We not only move beyond CIO's reporting structure to a focus on recently emerging digital upper echelons, i.e., CDOs and CISOs, but also complement the literature by examining more diverse reporting options—i.e., reporting to the IT head (e.g., often CIO or CTO in firms) versus non-IT head such as CEO or CFO.

Furthermore, our consideration of firms' strategic visions aligned with emerging digital upper echelons' reporting structure are also more state-of-art and relevant to the emerging leadership roles than previous studies. Research examining CIOs' reporting structure tends to focus on firms' generic strategies such as cost leadership and differentiation (e.g., Al-Taie et al., 2014; Banker et al., 2011; Karanja et al., 2021). We move beyond these generic firm strategies to focus on digital transformation and security awareness that are more directly relevant to CDOs and CISOs.

Our unique focus of firm strategic visions also contributes to the growing literature about digital transformation and firm security strategies. While prior studies have qualitatively recognized the tradeoffs in firms' digital transformation initiatives (e.g., Gaskin et al., 2014; Tabrizi et al., 2019; Tilson et al., 2010) and empirically demonstrated the positive impacts of digital transformation on firm performance (e.g., Chen & Srinivasan, 2023), this research extends our understanding with a new boundary condition—i.e., CDOs' reporting structure. We demonstrate that while digital transformation consistently improves firms' retrospective performance, its impacts on prospective performance are contingent on to whom the CDO reports. Hence, this research joins the conversation of digital transformation's impacts and highlights the importance of properly align digital transformation with CDOs' reporting structure.

While prior firm security research has highlighted the role of firm security awareness, the focused has been placed on its impacts on security breaches and investments in IT and/or security countermeasures (e.g., Li et al., 2023). This research moves beyond the security impacts to examine how firms' security awareness influence financial performance and its contingency on CISOs' reporting structure. We not only demonstrate the negative impacts of security awareness on firms' retrospective performance, but also indicate that having CISOs reporting to non-IT heads (i.e., cross-group reporting structure) can mitigate such negative impacts.

Practical Implications

This research informs governance choices faced by practitioners confronted with decisions about how to assemble teams of CDOs and CISOs to relatively more mature executives, such as CEOs, CFOs, COOs, and CIOs, to face the challenges of digital transformation and cybersecurity that pose opportunities and threats to firm performance. Our results highlight that CDOs' and CISOs' reporting structures should be aligned with the firm's strategic visions—i.e., digital transformation and security awareness. Firms with CDOs reporting to IT heads (i.e., within-group reporting structure) can achieve a stronger positive return from digital transformation. Firms are also advised to aware the negative impacts of security awareness on the short-term, operational performance (i.e., retrospective performance). One possible mitigation strategy is to have CISOs reporting to non-IT heads (i.e., across-group reporting structure).

Limitations and Future Research

We also acknowledge the limitations of this study and accordingly discuss future research opportunities. First, our sample only focuses on S&P 1500 firms. Although the S&P 1500 is representative and suitable for this research, future studies can replicate or extend our findings to other sets of firms. Opportunities of contextualizing our theoretical development also exist, where future research can identify how the impacts of CDOs' and CISOs' reporting structures vary in different contexts. Second, our theory focuses on CDOs and CISOs because of their prevalence, future research can examine other emerging digital upper echelons, such as chief data officers. Third, future research can extend our study using alternative categorization of reporting structure types. For example, studies can take a group perspective to theorize how the composition and dynamics of the group where CDOs and CISOs resides in affect firm performance.

CHAPTER 5

DISCUSSIONS AND CONCLUSION

Emerging digital upper echelons encompasses the exploration of novel approaches, skills, and mindsets required to navigate the intricate interplay between technology and business. It represents a departure from the “traditional” leadership model, as it incorporates a fast and deep understanding of emerging technologies, a keen eye for innovation, and the ability to harness the power of digital transformation. As organizations rely more heavily on technology for competitive advantages and sustainability, a better understanding of the emerging digital upper echelons becomes paramount to unpacking its full potential.

This three-essay dissertation serves as a starting point to systematically understand the sounding impacts of emerging digital upper echelons and the contingencies on how to govern them. In doing so, we provide important theoretical and practical implications.

Findings from the first essay advocate the innovation benefits of appointing a CISO to the TMT, which adds additional flavors to the established positive impacts of CISOs on firm security performance. Our results are also nuanced to advise firms on how to select CISOs in TMT with various backgrounds such as prior working experience and educations. Examining the impacts of CISO presence in TMT on firm innovation offers theoretical implications to both IT leadership and information security literature. First, our findings illustrate the business value of firms hiring CISOs to the TMT, which distinguishes our work from prior literature that focused on the security impacts of

CISOs. Second, a growing body of literature has qualitatively, or through self-report surveys, examined how technology-related TMT members, such as CIOs (Chen et al., 2021; Li et al., 2021; Leidner et al., 2010), CDOs (Tumbas et al., 2018) and Chief Data Officers (Lee et al., 2014), affect firm innovation. This essay adds to this stream of literature by demonstrating the impacts of an CISO in TMT on firm innovation through unique mechanisms. Finally, by illustrating how different CISO backgrounds, such as prior industry experience and educational background, impact firm innovation, we provide insight to managers seeking to hire CISOs to improve firm security and innovation performance.

The second essay demonstrates the significantly different impacts of digital upper echelons and non-digital upper echelons' compensation on the firm's timely disclosure of security breaches, offering fresh contributions to the literature on executive compensation and data breach disclosures. First, we extend the differing effects of agency incentives to the cybersecurity context and consider how the divergent role-based priorities and goals of different digital upper echelon groups can alter the influence of executive compensation on firms' strategic decisions. Second, prior literature generally finds that IT expertise at the board level benefits firms through increased stock values, more efficient IT utilization, and more timely information flows to investors; however, our results point to the potential downsides of board members' informal cybersecurity expertise on the board because it contributes to slower SEC notification. Third, this research contributes to the recent literature that examines why firms timely disclose data breaches by adding an executive compensation and board cybersecurity knowledge perspective.

The third essay delineates the advantages of CDOs' within-group reporting structure (i.e., reporting to IT heads) and CISOs' across-group reporting structure (i.e., reporting to non-IT heads) on amplifying the returns from firm strategic visions tied to their in-role responsibilities, i.e., digital transformation and security awareness, respectively. This essay extends our understanding to the contingent effects of emerging digital upper echelon's reporting structure on the firm performance. Our findings add insights to IT leadership literature by studying reporting structure of emerging digital upper echelons, i.e., CDOs and CISOs. Previous literature examines the performance of CIO reporting structure, i.e., reporting to CEO versus CFO, and their contingent impacts on the firm's strategic vision. We not only extend the reporting option for emerging digital upper echelons (i.e., CDOs and CISOs) to within versus across the digital upper echelon group, but also focus on the emerging strategic visions (i.e., digital transformation and security awareness) that are tied to the responsibilities of these emerging digital upper echelons. Findings from the third essay also contributes to the literature about digital transformation and security awareness by demonstrating how their impacts on firm performance are contingent on the corresponding digital upper echelons' reporting structure. Business managers are advised on how to properly design emerging digital upper echelons' reporting structure to maximize the emerging strategic visions' contributions to firm performance.

We acknowledge that this three-essay dissertation is only a starting point to unpack the impacts and governance of emerging digital upper echelons. A fruitful line of future research opportunities exists. We discuss some directions to guide future research.

First, in this dissertation, we focus on the appointment of emerging digital upper echelons to the TMT, their compensation, and their reporting structure. Future research can draw on the previous CEO and CIO literature that tackled each individual digital upper echelon's characteristics and conceptualize important characteristics of emerging IT leaders. For example, studies are needed to understand how CDOs' and CISOs' demographic attributes (e.g., gender), personality (e.g., political ideology, sensation seeking, overconfidence, military background), and experience (e.g., expertise, tenure) influence firm performance and strategic decisions. While these characteristics have been examined for CEOs and some of them have been studied for CIOs (e.g., You et al., 2020), future research can compare how the impacts of these characteristics are different for CDOs and CISOs.

Second, this dissertation, especially the third essay, has viewed the governance of emerging digital upper echelons as an important contingency on the firm's strategy-performance link. However, prior research has also identified organizational structure as the important driver of the firm's strategic orientation, innovation, and inter-functional (or inter-departmental) relationships (Lee et al., 2015). Accordingly, future research can examine the impacts of emerging IT leaders' reporting structure on firms' strategic orientation and competitive actions. Research also can be done to understand how the reporting structure of firms' emerging digital upper echelons help modularize the inter-functional collaborations and dynamics.

Third, this dissertation has separately investigated the impacts of each individual emerging digital upper echelon role, such as CDOs and CISOs. Future research can extend the individual role-based conceptualization to focus on the group-level study. For example, studies can view the emerging IT leader's group composition and dynamics over time to examine how the alignment between the emerging digital upper echelon and the group characteristics influence firm performance. It will also be worthy to investigate how emerging digital upper echelons reside in groups and trigger group dynamics within and across organizations.

Fourth, we have focused on the internal governance of emerging digital upper echelons within the firm's TMT. However, external board of directors and other stakeholders such as investors also play important roles in shaping the decisions of hiring and governing emerging digital upper echelons. Future research can examine how board of directors affect the effectiveness of appointing and governing emerging IT executives. Studies also can be done to understand how board of directors should effectively advise the firm's TMT, especially the position and expectations for emerging digital upper echelons.

In conclusion, this dissertation offers a starting point of examining emerging digital upper echelons' appointments, governances, and impacts. Future research can build on this dissertation to advance our understanding of emerging digital upper echelons further. We hope to motivate a cumulative tradition of research focusing on the changing landscape of digital upper echelons in organizations.

REFERENCES

Aljazzaf, S., Mithas, S., & Park, Y. (2019). The information technology reporting structure and firm performance: a configurational approach. In *Proceedings of the 2019 American Conference on Information Systems*.

Al-Taie, M., Lane, M., & Cater-Steel, A. (2014). The relationship between organisational strategic IT vision and CIO roles: one size does not fit all. *Australasian Journal of Information Systems*, 18(2), 59-89. https://doi.org/10.3127/ajis.v18i2.827

Amir, E., Levi, S., & Livne, T. (2018). Do firms underreport information on cyber-attacks? Evidence from capital markets. *Review of Accounting Studies*, 23, 1177-1206. https://doi.org/10.1007/s11142-018-9452-4

Arend, R. J., Zhao, Y. L., Song, M., & Im, S. (2017). Strategic planning as a complex and enabling managerial tool. *Strategic Management Journal*, 38(8), 1741-1752. https://doi.org/10.1002/smj.2420

Ashraf, M., Jiang, J. X., & Wang, I. Y. (2022). Are there trade-offs with mandating timely disclosure of cybersecurity incidents? Evidence from state-level data breach disclosure laws. *The Journal of Finance and Data Science*, 8, 202-213. https://doi.org/10.1016/j.jfds.2022.08.001

Bandodkar, N., & Grover, V. (2022). Does it pay to have CIOs on the board? Creating value by appointing C-level IT executives to the board of directors. *Journal of the Association for Information Systems*, 23(4), 838-888. https://doi.org/10.17705/1jais.00747

Banker, R. D., Hu, N., Pavlou, P. A., & Luftman, J. (2011). CIO reporting structure, strategic positioning, and firm performance. *MIS Quarterly*, 35(2), 487-504. https://doi.org/10.2307/23044053

Barth, M. E., & Schipper, K. (2008). Financial reporting transparency. *Journal of Accounting, Auditing & Finance*, 23(2), 173-190. https://doi.org/10.1177/0148558X0802300203

Bass, A. S. (2018). Non-tech businesses are beginning to use artificial intelligence at scale. *The Economist*, 3-5.

Bendig, D., Wagner, R., Jung, C., & Nüesch, S. (2022). When and why technology leadership enters the C-suite: An antecedents perspective on CIO presence. *The Journal of Strategic Information Systems*, 31(1), 101705. https://doi.org/10.1016/j.jsis.2022.101705

Berard, D. (2018). Kaspersky Lab Report: Data Breaches in North America Can Lead to C-Level Job Loss. *Kapersky Labs*. Retrieved March 2023 from https://usa.kaspersky.com/about/press-releases/2018_-kaspersky-lab-report-data-breaches-in-north-america-can-lead-to-c-level-job-loss

Bolster, P., Pantalone, C. H., & Trahan, E. A. (2010). Security breaches and firm value. *Journal of Business Valuation and Economic Loss Analysis*, 5(1). https://doi.org/10.2202/1932-9156.1081

Burt, R. S. (1980). Cooptive corporate actor networks: A reconsideration of interlocking directorates involving American manufacturing. *Administrative Science Quarterly*, 25(4), 557-582. https://doi.org/10.2307/2392281

Burt, R. S. (1992). Structural holes: The social structure of competition. *Harvard University Press*.

Carter, M., Grover, V., & Thatcher, J. B. (2011). The emerging CIO role of business technology strategist. *MIS Quarterly Executive*, 10(1), 19-29.

Chatterjee, D., Richardson, V. J., & Zmud, R. W. (2001). Examining the shareholder wealth effects of announcements of newly created CIO positions. *MIS Quarterly*, 25(1), 43-70. https://doi.org/10.2307/3250958

Chau, D. C., Ngai, E. W., Gerow, J. E., & Thatcher, J. B. (2020). The effects of business–IT strategic alignment and IT governance on firm performance: A moderated polynomial regression analysis. *MIS Quarterly*, 44(4), 1679-1703. https://doi.org/10.25300/MISQ/2020/12165

Chen, D. Q., Preston, D. S., & Xia, W. (2010). Antecedents and effects of CIO supply-side and demand-side leadership: A staged maturity model. *Journal of Management Information Systems*, 27(1), 231-272. https://doi.org/10.2753/MIS0742-1222270110

Chen, D. Q., Zhang, Y., Xiao, J., & Xie, K. (2021). Making digital innovation happen: a chief information officer issue selling perspective. *Information Systems Research*, 32(3), 987-1008. https://doi.org/10.1287/isre.2021.1008

Chen, W., & Srinivasan, S. (2023). Going digital: Implications for firm value and performance. *Review of Accounting Studies*, 1-47. https://doi.org/10.1007/s11142-023-09753-0

Cheng, Z., Rai, A., Tian, F., & Xu, S. X. (2021). Social learning in information technology investment: the role of board interlocks. *Management Science*, 67(1), 547-576. https://doi.org/10.1287/mnsc.2019.3548

Choi, I., Chung, S., Han, K., & Pinsonneault, A. (2021). CEO risk-taking incentives and IT innovation: The moderating role of a CEO's IT-related human capital. *MIS Quarterly*, 45(4), 2175-2192. https://doi.org/10.25300/MISQ/2022/15606

Chung, S., Animesh, A., Han, K., & Pinsonneault, A. (2019). Software patents and firm value: A real options perspective on the role of innovation orientation and environmental uncertainty. *Information Systems Research*, 30(3), 1073-1097. https://doi.org/10.1287/isre.2019.0854

Clò, S., Florio, M., & Rentocchini, F. (2020). Firm ownership, quality of government and innovation: Evidence from patenting in the telecommunication industry. *Research Policy*, 49(5), 103960. https://doi.org/10.1016/j.respol.2020.103960

Coles, J. L., Daniel, N. D., & Naveen, L. (2006). Managerial incentives and risk-taking. *Journal of Financial Economics*, 79(2), 431-468. https://doi.org/10.1016/j.jfineco.2004.09.004

Conyon, M. J. (2006). Executive compensation and incentives. *Academy of Management Perspectives*, 20(1), 25-44. https://doi.org/10.5465/amp.2006.19873408

Custódio, C., Ferreira, M. A., & Matos, P. (2013). Generalists versus specialists: Lifetime work experience and chief executive officer pay. *Journal of Financial Economics*, 108(2), 471-492. https://doi.org/10.1016/j.jfineco.2013.01.001

Custódio, C., Ferreira, M. A., & Matos, P. (2019). Do general managerial skills spur innovation?. *Management Science*, 65(2), 459-476. https://doi.org/10.1287/mnsc.2017.2828

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. https://doi.org/10.17705/1jais.00740

Dass, N., Kini, O., Nanda, V., Onal, B., & Wang, J. (2014). Board expertise: Do directors from related industries help bridge the information gap?. *The Review of Financial Studies*, 27(5), 1533-1592. https://doi.org/10.1093/rfs/hht071

Dawson, G. S., Denford, J. S., & Desouza, K. C. (2016). Governing innovation in US state government: An ecosystem perspective. *The Journal of Strategic Information Systems*, 25(4), 299-318. https://doi.org/10.1016/j.jsis.2016.08.003

Dawson, G. S., Ho, M. W., & Kauffman, R. J. (2015). How are C-suite executives different? A comparative empirical study of the survival of American chief information officers. *Decision Support Systems*, 74, 88-101. https://doi.org/10.1016/j.dss.2015.03.005

Devers, C. E., Cannella Jr, A. A., Reilly, G. P., & Yoder, M. E. (2007). Executive compensation: A multidisciplinary review of recent developments. *Journal of Management*, 33(6), 1016-1072. https://doi.org/10.1177/0149206307308588

Dezsö, C. L., & Ross, D. G. (2012). Does female representation in top management improve firm performance? A panel data investigation. *Strategic Management Journal*, 33(9), 1072-1089. https://doi.org/10.1002/smj.1955

Doan, M. (2019). Companies need to rethink what cybersecurity leadership is. *Harvard Business Review*.

Dokko, G., Wilk, S. L., & Rothbard, N. P. (2009). Unpacking prior experience: How career history affects job performance. *Organization Science*, 20(1), 51-68. https://doi.org/10.1287/orsc.1080.0357

Eisenhardt, K. M. (1989). Agency theory: An assessment and review. *Academy of Management Review*, 14(1), 57-74. https://doi.org/10.5465/amr.1989.4279003

Eklund, J. C., & Mannor, M. J. (2021). Keep your eye on the ball or on the field? Exploring the performance implications of executive strategic attention. *Academy of Management Journal*, 64(6), 1685-1713. https://doi.org/10.5465/amj.2019.0156

Engelen, A., Rieger, V., Wehner, M. C., & Heidemann, F. (2022). Is organizational commitment to IT good for employees? The role of industry dynamism and concentration. *MIS Quarterly*, 46(4), 2387-2404. https://doi.org/10.25300/MISQ/2022/16588

Enns, H. G., Huff, S. L., & Golden, B. R. (2001). How CIOs obtain peer commitment to strategic IS proposals: barriers and facilitators. *The Journal of Strategic Information Systems*, 10(1), 3-14. https://doi.org/10.1016/S0963-8687(01)00041-5

Feeny, D. F., & Willcocks, L. P. (1998). Core IS capabilities for exploiting information technology. *MIT Sloan Management Review*.

Feng, C., Patel, P. C., & Fay, S. (2021). The value of the structural power of the chief information officer in enhancing forward-looking firm performance. *Journal of Management Information Systems*, 38(3), 765-797. https://doi.org/10.1080/07421222.2021.1962599

Firk, S., Hanelt, A., Oehmichen, J., & Wolff, M. (2021). Chief digital officers: An analysis of the presence of a centralized digital transformation role. *Journal of Management Studies*, 58(7), 1800-1831. https://doi.org/10.1111/joms.12718

Fitzgerald, T. (2007). Clarifying the roles of information security: 13 questions the CEO, CIO, and CISO must ask each other. *Information Systems Security*, 16(5), 257-263. https://doi.org/10.1080/10658980701746577

Fitzgerald, M., Kruschwitz, N., Bonnet, D., & Welch, M. (2014). Embracing digital technology: A new strategic imperative. *MIT Sloan Management Review*, 55(2), 1-12.

Foerderer, J., & Schuetz, S. W. (2022). Data breach announcements and stock market reactions: a matter of timing?. *Management Science*, 68(10), 7298-7322. https://doi.org/10.1287/mnsc.2021.4264

Friedman, H. L. (2014). Implications of power: When the CEO can pressure the CFO to bias reports. *Journal of Accounting and Economics*, 58(1), 117-141. https://doi.org/10.1016/j.jacceco.2014.06.004

Gallino, S., & Rooderkerk, R. (2020). New product development in an omnichannel world. *California Management Review*, 63(1), 81-98. https://doi.org/10.1177/0008125620951969

Gaskin, J., Berente, N., Lyytinen, K., & Yoo, Y. (2014). Toward generalizable sociomaterial inquiry. *MIS Quarterly*, 38(3), 849-871. https://doi.org/10.25300/MISQ/2014/38.3.10

Ghule, K. (2020). As a CIO Do You Have a Plan If a Data Breach Occurs? *Cloud Anix*. https://www.cloudanix.com/blog/as-a-cio-do-you-have-a-plan-if-a-data-breach-occurs-at-your-organization/

Goh, B. W. (2009). Audit committees, boards of directors, and remediation of material weaknesses in internal control. *Contemporary Accounting Research*, 26(2), 549-579. https://doi.org/10.1506/car.26.2.9

Gordon, L. A., Loeb, M. P., & Sohail, T. (2010). Market value of voluntary disclosures concerning information security. *MIS Quarterly*, 567-594. https://doi.org/10.2307/25750692

Goyal, V. K., Lehn, K., & Racic, S. (2002). Growth opportunities and corporate debt policy: the case of the US defense industry. *Journal of Financial Economics*, 64(1), 35-59. https://doi.org/10.1016/S0304-405X(02)00070-3

Guldiken, O., Mallon, M. R., Fainshmidt, S., Judge, W. Q., & Clark, C. E. (2019). Beyond tokenism: How strategic leaders influence more meaningful gender diversity on boards of directors. *Strategic Management Journal*, 40(12), 2024-2046. https://doi.org/10.1002/smj.3049

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. https://doi.org/10.1080/07421222.2018.1451962

Hair Jr, J. F., Anderson, R. E., Tatham, R. L. & Black, W.C., (1995). Multivariate data analysis with readings, 3rd edn. *New York: Macmillan*.

Haislip, J. Z., Masli, A., Richardson, V. J., & Sanchez, J. M. (2016). Repairing organizational legitimacy following information technology (IT) material weaknesses: Executive turnover, IT expertise, and IT system upgrades. *Journal of Information Systems*, 30(1), 41-70. https://doi.org/10.2308/isys-51294

Haislip, J. Z., & Richardson, V. J. (2018). The effect of CEO IT expertise on the information environment: Evidence from earnings forecasts and announcements. *Journal of Information Systems*, 32(2), 71-94. https://doi.org/10.2308/isys-51796

Haislip, J. Z., Karim, K. E., Lin, K. J., & Pinsker, R. E. (2020). The influences of CEO IT expertise and board-level technology committees on Form 8-K disclosure timeliness. *Journal of Information Systems*, 34(2), 167-185. https://doi.org/10.2308/isys-52530

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. https://doi.org/10.1287/isre.2020.0986

Hambrick, D. C., & Mason, P. A. (1984). Upper echelons: The organization as a reflection of its top managers. *Academy of Management Review*, 9(2), 193-206. https://doi.org/10.5465/amr.1984.4277628

Hambrick, D. C., & Wowak, A. J. (2021). Strategic leadership. *Strategic Management: State of the Field and its Future*, 337-353.

Harris, J., & Bromiley, P. (2007). Incentives to cheat: The influence of executive compensation and firm performance on financial misrepresentation. *Organization Science*, 18(3), 350-367. https://doi.org/10.1287/orsc.1060.0241

Hartmann, C. C., & Carmenate, J. (2021). Academic research on the role of corporate governance and IT expertise in addressing cybersecurity breaches: implications for practice, policy, and research. *Current Issues in Auditing*, 15(2), A9-A23. https://doi.org/10.2308/CIIA-2020-034

Hausken, K. (2007). Information sharing among firms and cyber attacks. *Journal of Accounting and Public Policy*, 26(6), 639-688. https://doi.org/10.1016/j.jaccpubpol.2007.10.001

Heckman, J. J., & Robb Jr, R. (1985). Alternative methods for evaluating the impact of interventions: An overview. *Journal of Econometrics*, 30(1-2), 239-267. https://doi.org/10.1016/0304-4076(85)90139-3

Hess, T., Matt, C., Benlian, A., & Wiesböck, F. (2016). Options for formulating a digital transformation strategy. *MIS Quarterly Executive*, 15(2), 123-139.

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. https://doi.org/10.2308/isys-51402

Homroy, S., & Slechten, A. (2019). Do board expertise and networked boards affect environmental performance? *Journal of Business Ethics*, 158(1), 269-292. https://doi.org/10.1007/s10551-017-3769-y

Honoré, F. (2022). Joining forces: How can founding members' prior experience variety and shared experience increase startup survival?. *Academy of Management Journal*, 65(1), 248-272. https://doi.org/10.5465/amj.2018.1386

Hopkins, W. E., & Hopkins, S. A. (2002). Effects of cultural recomposition on group interaction processes. *Academy of Management Review*, 27(4), 541-553. https://doi.org/10.5465/amr.2002.7566059

Huang, C. D., Behara, R. S., & Goo, J. (2014). Optimal information security investment in a Healthcare Information Exchange: An economic analysis. *Decision Support Systems*, 61, 1-11. https://doi.org/10.1016/j.dss.2013.10.011

Johnson, A. M., & Lederer, A. L. (2005). The effect of communication frequency and channel richness on the convergence between chief executive and chief information officers. *Journal of Management Information Systems*, 22(2), 227-252. https://doi.org/10.1080/07421222.2005.11045842

Johnson, A. M., & Lederer, A. L. (2010). CEO/CIO mutual understanding, strategic alignment, and the contribution of IS to the organization. *Information & Management*, 47(3), 138-149. https://doi.org/10.1016/j.im.2010.01.002

Jones, M. C., Kappelman, L., Pavur, R., Nguyen, Q. N., & Johnson, V. L. (2020). Pathways to being CIO: The role of background revisited. *Information & Management*, 57(5), 103234. https://doi.org/10.1016/j.im.2019.103234

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. https://doi.org/10.1016/j.jfineco.2019.05.019

Kappelman, L., Johnson, V., Torres, R., Maurer, C., & McLean, E. (2019). A study of information systems issues, practices, and leadership in Europe. *European Journal of Information Systems*, 28(1), 26-42. https://doi.org/10.1080/0960085X.2018.1497929

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), 69-104.

Kappelman, L., McLean, E.R., Johnson, V.L., Torres, R., Maurer, C., Kim, K., Guerra, K. and Snyder, M., 2021. The 2020 SIM IT Issues and Trends Study. *MIS Quarterly Executive*, 20(1), 69-107.

Karahanna, E., & Preston, D. S. (2013). The effect of social capital of the relationship between the CIO and top management team on firm performance. *Journal of Management Information Systems*, 30(1), 15-56. https://doi.org/10.2753/MIS0742-1222300101

Karanja, E. (2017). The role of the chief information security officer in the management of IT security. *Information & Computer Security*, 25(3), 300-329. https://doi.org/10.1108/ICS-02-2016-0013

Karanja, E., Grant, D., & Zaveri, J. S. (2021). CIO reporting structure and firm strategic orientation–a content analysis approach. *Journal of Systems and Information Technology*, 23(1), 20-52. https://doi.org/10.1108/JSIT-02-2020-0022

Karyda, M., Kiountouzis, E., & Kokolakis, S. (2005). Information systems security policies: a contextual perspective. *Computers & Security*, 24(3), 246-260. https://doi.org/10.1016/j.cose.2004.08.011

Keats, B. W., & Hitt, M. A. (1988). A causal model of linkages among environmental dimensions, macro organizational characteristics, and performance. *Academy of Management Journal*, 31(3), 570-598. https://doi.org/10.5465/256460

Keizera, J. A., Halman, J. I., & Song, M. (2002). From experience: applying the risk diagnosing methodology. *Journal of Product Innovation Management*, 19(3), 213-232. https://doi.org/10.1111/1540-5885.1930213

Kim, K., Ok, C., Kang, S. C., Bae, J., & Kwon, K. (2021). Highp-erformance work systems with internal and external contingencies: the moderating roles of organizational slack and industry instability. *Human Resource Management*, 60(3), 415-433. https://doi.org/10.1002/hrm.22030

Kim, K., Lee, J., & Gopal, A. (2021). Soft but Strong: Software-Based Innovation and Product Differentiation in the IT Hardware Industry. *MIS Quarterly*, 46(2), 1273-1294. https://doi.org/10.25300/MISQ/2022/16517

Kini, O., Kracaw, W., & Mian, S. (2004). The nature of discipline by corporate takeovers. *The Journal of Finance*, 59(4), 1511-1552. https://doi.org/10.1111/j.1540-6261.2004.00671.x

Kogan, L., Papanikolaou, D., Seru, A., & Stoffman, N. (2017). Technological innovation, resource allocation, and growth. *The Quarterly Journal of Economics*, 132(2), 665-712. https://doi.org/10.1093/qje/qjw040

Kohli, R., Devaraj, S., & Ow, T. T. (2012). Does information technology investment influence a firm's market value? A case of non-publicly traded healthcare firms. *MIS Quarterly*, 36(4), 1145-1163. https://doi.org/10.2307/41703502

Kronlund, M., & Sandy, S. (2014). Does shareholder scrutiny affect executive compensation? Evidence from say-on-pay voting. Evidence from Say-on-Pay Voting. Working paper.

Kwon, J., & Johnson, M. E. (2014). Proactive versus reactive security investments in the healthcare sector. *MIS Quarterly*, 38(2), 451-471. https://doi.org/10.25300/MISQ/2014/38.2.06

Lee, J. Y., Kozlenkova, I. V., & Palmatier, R. W. (2015). Structural marketing: Using organizational structure to achieve marketing objectives. *Journal of the Academy of Marketing Science*, 43(1), 73-99. https://doi.org/10.1007/s11747-014-0402-9

Lee, Y., Madnick, S., Wang, R., Wang, F., & Zhang, H. (2014). A cubic framework for the chief data officer: Succeeding in a world of big data. *MIS Quarterly Executive*, 13(1), 1-13.

Leidner, D. E., Preston, D., & Chen, D. (2010). An examination of the antecedents and consequences of organizational IT innovation in hospitals. *Journal of Strategic Information Systems*, 19(3), 154-170. https://doi.org/10.1016/j.jsis.2010.07.002

Lerman, A., & Livnat, J. (2010). The new Form 8-K disclosures. *Review of Accounting Studies*, 15(4), 752-778. https://doi.org/10.1007/s11142-009-9114-7

Li, H., Wu, Y., Cao, D., & Wang, Y. (2021). Organizational mindfulness towards digital transformation as a prerequisite of information processing capability to achieve market agility. *Journal of Business Research*, 122(C), 700-712. https://doi.org/10.1016/j.jbusres.2019.10.036

Li, H., Yoo, S., & Kettinger, W. J. (2021). The Roles of IT Strategies and Security Investments in Reducing Organizational Security Breaches. *Journal of Management Information Systems*, 38(1), 222-245. https://doi.org/10.1080/07421222.2021.1870390

Li, J., Li, M., Wang, X., & Thatcher, J. B. (2021). Strategic directions for AI: The role of CIOs and boards of directors. *MIS Quarterly*, 45(3), 1603-1643. https://doi.org/10.25300/MISQ/2021/16523

Li, M., & Ye, L. R. (1999). Information technology and firm performance: Linking with environmental, strategic and managerial contexts. *Information & Management*, 35(1), 43-51. https://doi.org/10.1016/S0378-7206(98)00075-5

Li, W., Leung, A. & Yue, W. T. (2023). Where is IT in information security? The interrelationship among IT investment, security awareness, and data breaches. *MIS Quarterly*, 47(1), 317-342. https://doi.org/10.25300/misq/2022/15713

Lin, A., & Chen, N. C. (2012). Cloud computing as an innovation: Perception, attitude, and adoption. *International Journal of Information Management*, 32(6), 533-540. https://doi.org/10.1016/j.ijinfomgt.2012.04.001

Lin, Z., Sapp, T. R. A., Ulmer, J. R., & Parsa, R. (2020). Insider trading ahead of cyber breach announcements. *Journal of Financial Markets*, 50(C), 100527. https://doi.org/10.1016/j.finmar.2019.100527

Liu, X. K., & Preston, D. S. (2021). The Chief Information Officer: Impact on Organizational Forecasting Outcomes. *Journal of the Association for Information Systems*, 22(4), 968-1006. https://doi.org/10.17705/1jais.00686

Livengood, R. S., & Reger, R. K. (2010). That's our turf! Identity domains and competitive dynamics. *Academy of Management Review*, 35(1), 48-66. https://doi.org/10.5465/amr.35.1.zok48

Lyngsie, J., & Foss, N. J. (2017). The more, the merrier? Women in top-management teams and entrepreneurship in established firms. *Strategic Management Journal*, 38(3), 487-505. https://doi.org/10.1002/smj.2510

Makridis, C. A. (2021). Do data breaches damage reputation? Evidence from 45 companies between 2002 and 2018. *Journal of Cybersecurity*, 7(1), 1-8. https://doi.org/10.1093/cybsec/tyab021

Maner, J. K., Miller, S. L., Moss, J. H., Leo, J. L., & Plant, E. A. (2012). Motivated social categorization: fundamental motives enhance people's sensitivity to basic social categories. *Journal of Personality and Social Psychology*, 103(1), 70-83. https://doi.org/10.1037/a0028172

Mao, C. X., & Weathers, J. (2019). Employee treatment and firm innovation. *Journal of Business Finance & Accounting*, 46(7-8), 977-1002. https://doi.org/10.1111/jbfa.12393

Marquis, C., & Tilcsik, A. (2016). Institutional equivalence: How industry and community peers influence corporate philanthropy. *Organization Science*, 27(5), 1325-1341. https://doi.org/10.1287/orsc.2016.1083

Maruca, R. F. (2000). Are CIOs Obsolete?. *Harvard Business Review*, 78(2), 55-55.

Maynard, S., Onibere, M., & Ahmad, A. (2018). Defining the strategic role of the chief information security officer. *Pacific Asia Journal of the Association for Information Systems*, 10(3), 61-85. https://doi.org/10.17705/1pais.10303

Menz, M. (2012). Functional top management team members: A review, synthesis, and research agenda. *Journal of Management*, 38(1), 45-80. https://doi.org/10.1177/0149206311421830

Menz, M., & Scheef, C. (2014). Chief strategy officers: Contingency analysis of their presence in top management teams. *Strategic Management Journal*, 35(3), 461-471. https://doi.org/10.1002/smj.2104

Messersmith, J. G., Lee, J. Y., Guthrie, J. P., & Ji, Y. Y. (2014). Turnover at the top: Executive team departures and firm performance. *Organization Science*, 25(3), 776-793. https://doi.org/10.1287/orsc.2013.0864

Metzler, D. R., Bankamp, S., Muntermann, J., & Palmer, M. (2021). The Role of CDOs in signaling digital transformation endeavors: An analysis of firms' external communication tools. In *Proceedings of the 42nd International Conference on Information Systems*.

Meyer, A. D., Brooks, G. R., & Goes, J. B. (1990). Environmental jolts and industry revolutions: Organizational responses to discontinuous change. *Strategic Management Journal*, 11, 93-110.

Milbourn, T. T. (2003). CEO reputation and stock-based compensation. *Journal of Financial Economics*, 68(2), 233-262. https://doi.org/10.1016/S0304-405X(03)00066-7

Mithas, S., Tafti, A., & Mitchell, W. (2013). How a firm's competitive environment and digital strategic posture influence digital business strategy. *MIS Quarterly*, 37(2), 511-536. https://doi.org/10.25300/MISQ/2013/37.2.09

Morgan, S. (2020). Pink Slips to Million Dollar Salaries: Are CISOs Underappreciated or Overpaid? *Cybercrime Magazine*. Retrieved December 9, 2021 from https://cybersecurityventures.com/pink-slips-to-million-dollar-salaries-are-cisos-underappreciated-or-overpaid/

Nash/KPMG, H. (2018). CIO Survey 2018: The Transformational CIO. https://assets.kpmg/content/dam/kpmg/xx/pdf/2018/06/harvey-nash-kpmg-cio-survey-2018.pdf

Nath, P., & Mahajan, V. (2008). Chief marketing officers: A study of their presence in firms' top management teams. *Journal of Marketing*, 72(1), 65-81. https://doi.org/10.1509/jmkg.72.1.065

Nath, P., & Bharadwaj, N. (2020). Chief marketing officer presence and firm performance: Assessing conditions under which the presence of other C-level functional executives matters. *Journal of the Academy of Marketing Science*, 48(4), 670-694. https://doi.org/10.1007/s11747-019-00714-1

Neumann, S., & Zviran, M. (1997). Tel Aviv City hall—The computerization revolution. *The Journal of Strategic Information Systems*, 6(2), 149-167. https://doi.org/10.1016/S0963-8687(97)00011-5

Neville-Neil, G. V. (2019). What is a chief security officer good for?. *Communications of the ACM*, 62(10), 26-27. https://doi.org/10.1145/3357227

Nicholson, G., & Newton, C. (2010). The role of the board of directors: Perceptions of managerial elites. *Journal of Management and Organization*, 16(2), 204-218. https://doi.org/10.5172/jmo.16.2.204

Osborne, S. P., & Flemig, S. S. (2015). Conceptualizing risk and social innovation: An integrated framework for risk governance. *Society and Economy*, 37(2), 165-182. https://doi.org/10.1556/204.2015.37.2.2

Prattipati, S. N., & Mensah, M. O. (1997). Information systems variables and management productivity. *Information & Management*, 33(1), 33-43. https://doi.org/10.1016/S0378-7206(97)00036-0

Preston, D. S., & Karahanna, E. (2009a). Antecedents of IS strategic alignment: a nomological network. *Information Systems Research*, 20(2), 159-179. https://doi.org/10.1287/isre.1070.0159

Preston, D., & Karahanna, E. (2009b). How to develop a shared vision: The key to IS strategic alignment. *MIS Quarterly Executive*, 8(1), 1-8.

Quinn, K. A., & Macrae, C. N. (2005). Categorizing others: the dynamics of person construal. *Journal of Personality and Social Psychology*, 88(3), 467-479. https://doi.org/10.1037/0022-3514.88.3.467

Ratner, K. G., Dotsch, R., Wigboldus, D. H., van Knippenberg, A., & Amodio, D. M. (2014). Visualizing minimal ingroup and outgroup faces: implications for impressions, attitudes, and behavior. *Journal of Personality and Social Psychology*, 106(6), 897-911. https://doi.org/10.1037/a0036498

Richard, O. C., Wu, J., Markoczy, L. A., & Chung, Y. (2019). Top management team demographic-faultline strength and strategic change: What role does environmental dynamism play?. *Strategic Management Journal*, 40(6), 987-1009. https://doi.org/10.1002/smj.3009

Riemenschneider, C. K., & Armstrong, D. J. (2021). The Development of the Perceived Distinctiveness Antecedent of Information Systems Professional Identity. *MIS Quarterly*, 45(3a), 1149-1186. https://doi.org/10.25300/MISQ/2021/14626

Roh, J., Krause, R., & Swink, M. (2016). The appointment of chief supply chain officers to top management teams: A contingency model of firm-level antecedents and consequences. *Journal of Operations Management*, 44(1), 48-61. https://doi.org/10.1016/j.jom.2016.05.001

Rose, A. M. (2021). A response to calls for SEC-mandated ESG disclosure. Washington University Law Review, 98(6), 1821-1857.

Ross, S. A. (1973). The economic theory of agency: The principal's problem. *American Economic Review*, 63(2), 134-139.

Rule, N. O., Garrett, J. V., & Ambady, N. (2010). Places and faces: Geographic environment influences the ingroup memory advantage. *Journal of Personality and Social Psychology*, 98(3), 343-355. https://doi.org/10.1037/a0018589

Sanders, W. G., & Hambrick, D. C. (2007). Swinging for the fences: The effects of CEO stock options on company risk taking and performance. *Academy of Management Journal*, 50(5), 1055-1078. https://doi.org/10.5465/amj.2007.27156438

SEC. (2018). Securities and exchange commission 17 CFR parts 240 and 249 release No. 34-64976; File No. S7-10-10.

Shayo, C., & Lin, F. (2019). An Exploration of the Evolving Reporting Organizational Structure for the Chief Information Security Officer (CISO) Function. *Journal of Computer Science*, 7(1), 1-20. https://doi.org/10.15640/jcsit.v7n1a1

Shumsky, T. (2016). Corporate Judgment Call: When to Disclose You've Been Hacked. *The Wall Street Journal*. Retrieved December 9, 2021 from https://www.wsj.com/articles/corporate-judgment-call-when-to-disclose-youve-been-hacked-1474320689

Singh, A., & Hess, T. (2017). How chief digital officers promote the digital transformation of their companies. MIS Quarterly Executive, 16(1), 1-17.

Sobol, M. G., & Klein, G. (2009). Relation of CIO background, IT infrastructure, and economic performance. *Information & Management*, 46(5), 271-278. https://doi.org/10.1016/j.im.2009.05.001

Srinivasan, S. (2005). Consequences of financial reporting failure for outside directors: Evidence from accounting restatements and audit committee members. *Journal of Accounting Research*, 43(2), 291-334. https://doi.org/10.1111/j.1475-679x.2005.00172.x

Stangor, C., Lynch, L., Duan, C., & Glas, B. (1992). Categorization of individuals on the basis of multiple social features. *Journal of Personality and Social Psychology*, 62(2), 207. https://doi.org/10.1037/0022-3514.62.2.207

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(C), 15-29. https://doi.org/10.1016/j.aos.2018.04.005

Tabrizi, B., Lam, E., Girard, K., & Irvin, V. (2019). Digital transformation is not about technology. *Harvard Business Review*, 13(March), 1-6.

Tai, L. A., & Phelps, R. (2000). CEO and CIO perceptions of information systems strategy: evidence from Hong Kong. *European Journal of Information Systems*, 9(3), 163-172. https://doi.org/10.1057/palgrave.ejis.3000362

Taylor, J., & Vithayathil, J. (2018). Who delivers the bigger bang for the buck: CMO or CIO?. *The Journal of Strategic Information Systems*, 27(3), 207-220. https://doi.org/10.1016/j.jsis.2018.04.001

Tchetgen, E. J. T., Walter, S., Vansteelandt, S., Martinussen, T., & Glymour, M. (2015). Instrumental variable estimation in a survival context. *Epidemiology*, 26(3), 402-410. https://doi.org/10.1097/EDE.0000000000000262

Teodoridis, F., Bikard, M., & Vakili, K. (2019). Creativity at the knowledge frontier: The impact of specialization in fast-and slow-paced domains. *Administrative Science Quarterly*, 64(4), 894-927. https://doi.org/10.1177/0001839218793384

Tesluk, P. E., & Jacobs, R. R. (1998). Toward an integrated model of work experience. *Personnel Psychology*, 51(2), 321-355. https://doi.org/10.1111/j.1744-6570.1998.tb00728.x

Tilson, D., Lyytinen, K., & Sørensen, C. (2010). Digital infrastructures: The missing IS research agenda. *Information Systems Research*, 21(4), 748-759. https://doi.org/10.1287/isre.1100.0318

Tosun, O. K. (2021). Cyber-attacks and stock market activity. *International Review of Financial Analysis*, 76(C), 101795. https://doi.org/10.1016/j.irfa.2021.101795

Tsai, C. H., & Su, P. C. (2021). The application of multi-server authentication scheme in internet banking transaction environments. *Information Systems and E-Business Management*, 19(1), 77-105. https://doi.org/10.1007/s10257-020-00481-5

Tumbas, S., Berente, N., & Brocke, J. V. (2018). Digital innovation and institutional entrepreneurship: Chief digital officer perspectives of their emerging role. *Journal of Information Technology*, 33(3), 188-202. https://doi.org/10.1057/s41265-018-0055-0

Vance, A., Lowry, M. R., & Sahin, Z., (2022). Taking a Seat at the Table: The Quest for CISO Legitimacy. In *Proceedings of the 43rd International Conference on Information Systems*.

Vincent, N. E., Higgs, J. L., & Pinsker, R. E. (2017). IT governance and the maturity of IT risk management practices. *Journal of Information Systems*, 31(1), 59-77. https://doi.org/10.2308/isys-51365

Wagner, H. T., & Meshtaf, J. (2016). Individual IT roles in business-IT alignment and IT governance. In *Proceedings of the 49th Hawaii International Conference on System Sciences (HICSS)*, 4920-4929. https://doi.org/10.1109/HICSS.2016.610

Wang, C., Xie, F., & Zhu, M. (2015). Industry expertise of independent directors and board monitoring. *Journal of Financial and Quantitative Analysis*, 50(5), 929-962. https://doi.org/10.1017/S0022109015000459

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. https://doi.org/10.1287/isre.1120.0437

Watts, S., & Henderson, J. C. (2006). Innovative IT climates: CIO perspectives. *Journal of Strategic Information Systems*, 15(2), 125-151. https://doi.org/10.1016/j.jsis.2005.08.001

Westphal, J. D., & Zajac, E. J. (1994). Substance and Symbolism in CEOs' Long-Term Incentive Plans. *Administrative Science Quarterly*, 39(3), 367-390. https://doi.org/10.2307/2393295

Witschel, D., Döhla, A., Kaiser, M., Voigt, K. I., & Pfletschinger, T. (2019). Riding on the wave of digitization: Insights how and under what settings dynamic capabilities facilitate digital-driven business model change. *Journal of Business Economics*, 89(8), 1023-1095. https://doi.org/10.1007/s11573-019-00950-5

Wooldridge, J. M. (2010). Econometric analysis of cross section and panel data. *MIT Press*.

Wowak, A. J., Gomez-Mejia, L. R., & Steinbach, A. L. (2017). Inducements and motives at the top: A holistic perspective on the drivers of executive behavior. *Academy of Management Annals*, 11(2), 669-702. https://doi.org/10.5465/annals.2015.0121

Xiao, T., Makhija, M., & Karim, S. (2022). A knowledge recombination perspective of innovation: Review and new research directions. *Journal of Management*, 48(6), 1724-1777. https://doi.org/10.1177/01492063211055982

Xue, L., Ray, G., & Gu, B. (2011). Environmental uncertainty and IT infrastructure governance: A curvilinear relationship. *Information Systems Research*, 22(2), 389-399. https://doi.org/10.1287/isre.1090.0269

Xue, L., Ray, G., & Sambamurthy, V. (2012). Efficiency or innovation: How do industry environments moderate the effects of firms' IT asset portfolios?. *MIS Quarterly*, 36(2), 509-528. https://doi.org/10.2307/41703465

Yang, C., Huang, Q., Li, Z., Liu, K., & Hu, F. (2017). Big data and cloud computing: Innovation opportunities and challenges. *International Journal of Digital Earth*, 10(1), 13-53. https://doi.org/10.1080/17538947.2016.1239771

Yayla, A. A., & Hu, Q. (2014). The effect of board of directors' IT awareness on CIO compensation and firm performance. *Decision Sciences*, 45(3), 401-436. https://doi.org/10.1111/deci.12077

You, Y., Srinivasan, S., Pauwels, K., & Joshi, A. (2020). How CEO/CMO characteristics affect innovation and stock returns: Findings and future directions. *Journal of the Academy of Marketing Science*, 48(6), 1229-1253. https://doi.org/10.1007/s11747-020-00732-4

Young, S. (2013). Contemplating Corporate Disclosure Obligations Arising from Cybersecurity Breaches. *Journal of Corporation Law*, 38(3), 659-679.

Zadelhoff, M. V., (2017). Cybersecurity has a serious talent shortage. Here's how to fix it. *Harvard Business Review*, 5.

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. https://doi.org/10.1007/s10796-015-9562-5

Zajac, E. J., & Westphal, J. D. (1994). The costs and benefits of managerial incentives and monitoring in large US corporations: When is more not better? *Strategic Management Journal*, 15(S1), 121-142. https://doi.org/10.1002/smj.4250150909

Zhong, W., Ma, Z., Tong, T. W., Zhang, Y., & Xie, L. (2021). Customer concentration, executive attention, and firm search behavior. *Academy of Management Journal*, 64(5), 1625-1647. https://doi.org/10.5465/amj.2017.0468

APPENDIX A

Correlation Table of CISO Presence Paper

Variables	1	2	3	4	5	6	7	8	9	10	11	12
1. *Innovation*												
2. *CISOTMT*	0.19*											
3. *SpecialistCISOTMT*	0.18*	0.61*										
4. *GeneralistCISOTMT*	0.10*	0.77*	-0.04*									
5. *FirmSize*	0.24*	0.24*	0.16*	0.17*								
6. *Profitability*	0.04*	0.02*	0.02*	0.02*	0.03*							
7. *Leverage*	0.00	0.00	0.00	0.00	-0.01*	0.00						
8. *AssetTangibility*	-0.12*	-0.06*	-0.03*	-0.05*	0.07*	-0.01*	0.00					
9. *Capital Expenditure*	-0.03*	-0.04*	-0.02*	-0.03*	-0.07*	-0.03*	0.00	0.59*				
10. *R&DExpenditure*	0.30*	-0.00	0.02*	-0.02*	-0.26*	-0.15*	0.00	-0.19*	-0.06*			
11. *TechOfficer*	0.05*	-0.27*	-0.17*	-0.21*	0.10*	0.02*	0.00	-0.01*	-0.02*	-0.01		
12. *CROPresence*	-0.08*	0.13*	0.05*	0.12*	0.32*	-0.02*	-0.00	-0.13*	-0.12*	-0.14*	0.03*	
13. *CInnOPresence*	0.06*	0.14*	0.06*	0.12*	0.13*	0.02*	0.00	-0.01	-0.01*	-0.01	0.07*	0.03*
14. *FirmAge*	0.13*	0.06*	0.04*	0.04*	0.35*	0.06*	-0.00	0.15*	-0.02*	-0.07*	0.10*	0.08*
15. *GrowthOpportunity*	0.00	0.00	0.00	0.00	-0.04*	0.01*	0.00	-0.01*	0.00	0.02*	-0.01	-0.01*
16. *IndustryTurbulence*	0.05*	0.03*	0.02*	0.02*	-0.09*	-0.04*	-0.00	-0.07*	0.01*	0.13*	-0.02*	-0.07*
17. *MarketConcentration*	-0.06*	0.02*	0.01*	0.02*	-0.05*	0.04*	0.00	0.12*	0.08*	-0.10*	0.03*	-0.09*
18. *IndustryGrowth*	-0.02*	-0.01*	-0.01*	-0.01	-0.02*	0.01*	0.00	0.04*	0.01*	-0.02*	-0.00	-0.01*

Variables	13	14	15	16	17
14. *FirmAge*	0.07*				
15. *GrowthOpportunity*	0.00	-0.02*			
16. *IndustryTurbulence*	0.01*	-0.11*	0.01*		
17. *MarketConcentration*	0.07*	-0.05*	0.00	0.08*	
18. *IndustryGrowth*	0.00	0.00	0.00	-0.02*	0.14*

Notes: Number of observations: 70650; $*p < 0.05$.

APPENDIX B

Results of Two-Stage Least Square Model

Variables	Coefficient
CISOPresence	4.842** (0.043)
FirmSize	0.029 (0.046)
Profitability	0.044 (0.122)
Leverage	0.192*** (0.042)
AssetTangibility	0.235 (0.193)
CapitalExpenditure	-0.305 (0.212)
R&DExpenditure	2.282 (1.559)
TechOfficer	1.099** (0.531)
CROPresence	-0.138 (0.102)
CInnOPresence	-0.147 (0.112)
FirmAge	0.006 (0.123)
GrowthOpportunity	-0.000 (0.000)
IndustryTurbulence	-0.008 (0.216)
MarketConcentration	0.028 (0.592)
IndustryGrowth	0.349 (0.222)
Firm Fixed Effects	Yes
Quarter Fixed Effects	Yes

Notes: Number of observations: 70650; Significance levels: $^{*}p < 0.1$, $^{**}p < 0.05$, $^{***}p < 0.01$; Cluster standard errors are in parentheses.

APPENDIX C

Measurement of Risk-Seeking Incentive – Vega

Vega has been used to measure the risk-seeking incentive of the executive (Coles et al., 2006, Choi et al., 2021). Following code disclosed by one of the authors of Coles et al. (2006), Lalitha Naveen, we have replicated the calculation of Vega and get 99% correlation between our Vega and theirs. Here we briefly introduce how Vega is calculated. Vega is the partial derivative of the executive's option value estimated through Black-Scholes's option valuation model with respect to stock volatility.

The executive's option value model is as follow:

$$V = se^{-dT}N(Z) - Ke^{-rT}N(Z - \sigma\sqrt{T}) \qquad \text{C(1)}$$

Where s is the stock price at fiscal year end. T is the maturity option years. d indicates expected dividend yield, which is calculated by the average of the last three-year dividend yield, and dividend yield is the ratio of dividends per share to the close stock price. $N(Z)$ means the cumulative normal distribution function of Z and $Z = \frac{\log\left(\frac{S}{K}\right)+T\left(r-d+\frac{\sigma^2}{2}\right)}{\sigma\sqrt{T}}$. K is the strike price of the option. r indicates the risk-free rate of the corresponding maturity option years, which is disclosed by Federal Reserve System. σ is stock volatility, which is calculated by the annualized standard deviation of the monthly stock price in last 60 months before the beginning of the fiscal period multiple square root of 12. Both stock volatility and expected dividend yields are winsorized at 5 percentile and 95 percentile level.

The executive's risk-seeking incentive Vega equation is the partial derivate of equation C(1) with respect to stock volatility σ, therefore the equation is as follow:

$$Vega = \frac{\partial V}{\partial \sigma} = \frac{e^{-dT} N'(Z) S \sqrt{T}}{100} \qquad C(2)$$

where $N'(Z)$ is Z's normal density function.

The following is a table summarizing the results of mechanism tests.

	(1)	(2)	(3)
Variables	**Innovation**	**Innovation**	**Innovation**
CISOTMT × TMTRiskPreference	-0.0003*		
	(0.0002)		
CISOTMT × CommitmentToIT		-0.001	
		(0.007)	
CISOTMT × SecurityAwareness			-0.028*
			(0.014)
CISOTMT	0.099**	0.081**	0.080**
	(0.039)	(0.039)	(0.039)
TMTRiskPreference	0.001***	0.000***	0.000***
	(0.000)	(0.000)	(0.000)
CommitmentToIT	0.008***	0.008***	0.008***
	(0.002)	(0.002)	(0.002)
SecurityAwareness	0.003	0.003	0.007
	(0.004)	(0.004)	(0.005)
FirmSize	0.078***	0.080***	0.080***
	(0.018)	(0.018)	(0.018)
Profitability	-0.093	-0.091	-0.091
	(0.061)	(0.061)	(0.061)
Leverage	0.135***	0.138***	0.140***
	(0.025)	(0.025)	(0.026)
AssetTangibility	0.236**	0.238**	0.237**
	(0.094)	(0.094)	(0.094)
CapitalExpenditure	-0.049	-0.047	-0.046
	(0.091)	(0.090)	(0.090)
R&DExpenditure	2.139**	2.141**	2.139**
	(0.847)	(0.846)	(0.846)
TechOfficer	0.039***	0.040***	0.040***
	(0.015)	(0.015)	(0.015)
CROPresence	0.005	0.006	0.006
	(0.024)	(0.025)	(0.025)
CInnOPresence	0.004	0.008	0.008
	(0.035)	(0.035)	(0.035)
FirmAge	0.146***	0.152***	0.151***
	(0.034)	(0.034)	(0.034)
GrowthOpportunity	0.000*	0.000*	0.000*
	(0.000)	(0.000)	(0.000)
IndustryTurbulence	0.247***	0.248***	0.248***
	(0.091)	(0.090)	(0.090)

MarketConcentration	-0.127	-0.133	-0.134
	(0.217)	(0.216)	(0.216)
IndustryGrowth	0.082	0.080	0.078
	(0.077)	(0.077)	(0.077)
Firm Fixed Effects	Yes	Yes	Yes
Quarter Fixed Effects	Yes	Yes	Yes
R^2	0.114	0.113	0.113

Notes: Number of observations: 70650; Significance levels: *$p < 0.1$, **$p < 0.05$, ***$p < 0.01$; Clustered standard errors are in parentheses.

APPENDIX D

Results of Falsification Tests

Variables	(1)	(2) 4 quarters	(3) 5 quarters	(4) 6 quarters	(5) 7 quarters	(6) 8 quarters
MidSecManager	-0.016					
	(0.051)					
CISOTMTTurnover		-0.108*	-0.113**	-0.111**	-0.112**	-0.112**
		(0.055)	(0.055)	(0.055)	(0.055)	(0.056)
FirmSize	0.085***	0.085***	0.085***	0.085***	0.085***	0.085***
	(0.018)	(0.018)	(0.018)	(0.018)	(0.018)	(0.018)
Profitability	-0.089	-0.090	-0.091	-0.091	-0.091	-0.091
	(0.062)	(0.062)	(0.062)	(0.062)	(0.062)	(0.062)
Leverage	0.150***	0.150***	0.150***	0.150***	0.150***	0.150***
	(0.028)	(0.028)	(0.028)	(0.028)	(0.028)	(0.028)
AssetTangibility	0.241**	0.241**	0.242**	0.242**	0.242**	0.242**
	(0.094)	(0.094)	(0.094)	(0.094)	(0.094)	(0.094)
CapitalExpenditure	-0.042	-0.042	-0.042	-0.042	-0.042	-0.042
	(0.091)	(0.091)	(0.091)	(0.091)	(0.091)	(0.091)
R&DExpenditure	2.173**	2.164**	2.165**	2.166**	2.168**	2.170**
	(0.850)	(0.849)	(0.849)	(0.849)	(0.849)	(0.849)
TechOfficer	0.025	0.027*	0.028*	0.028*	0.029*	0.030*
	(0.016)	(0.016)	(0.016)	(0.016)	(0.016)	(0.016)
CROPresence	0.009	0.009	0.009	0.010	0.010	0.010
	(0.025)	(0.024)	(0.024)	(0.024)	(0.024)	(0.024)
CInnOPresence	0.001	0.001	0.001	0.001	0.001	0.001
	(0.036)	(0.036)	(0.036)	(0.036)	(0.036)	(0.036)
FirmAge	0.170***	0.169***	0.169***	0.169***	0.169***	0.169***
	(0.035)	(0.035)	(0.035)	(0.035)	(0.035)	(0.035)
GrowthOpportunity	0.000**	0.000**	0.000**	0.000**	0.000**	0.000**

	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)
IndustryTurbulence	0.256***	0.256***	0.255***	0.255***	0.255***	0.255***
	(0.094)	(0.095)	(0.095)	(0.095)	(0.095)	(0.095)
MarketConcentration	-0.145	-0.140	-0.139	-0.138	-0.138	-0.138
	(0.218)	(0.218)	(0.218)	(0.218)	(0.218)	(0.218)
IndustryGrowth	0.075	0.076	0.076	0.076	0.076	0.075
	(0.077)	(0.077)	(0.077)	(0.077)	(0.077)	(0.077)
Firm Fixed Effects	Yes	Yes	Yes	Yes	Yes	Yes
Quarter Fixed Effects	Yes	Yes	Yes	Yes	Yes	Yes
R^2	0.106	0.106	0.106	0.106	0.107	0.107

Notes: Number of observations: 70650; Significance levels: *$p < 0.1$, **$p < 0.05$, ***$p < 0.01$; Cluster standard errors are in parentheses.

APPENDIX E

Coding of CISO Educational Background

We collected LinkedIn profile data by searching on Google using "linkedin.com/in" + CISO's full name (i.e., first and last name) + "security". We saved the top 10 results for each search. One author of the paper and one research assistant have independently verified each record if the CISO has worked in this S&P 1500 firm in the data and reached an agreement. For records that did not have matched results, we manually searched them in Google with CISO's full name and the company names that the CISO has worked. In this process, we identified 418 CISO LinkedIn profiles among a total of 468 CISOs.

We gathered CISO's educational background through "education" section on LinkedIn pages, including degree and major. We manually coded each education experience (i.e., bachelor, master, and doctoral) as IT, business, legal/criminology, and STEM. Table D1 presents the coding schema and the number of CISOs for each category of educational background. Note that one CISO can have multiple majors. For example, they can have IS major for undergraduate and MBA for a master's degree. The following tables include a summary of CISO in TMT's educational background and effects of CISO educational background and industry experience on innovation.

Educational Background	Degrees and Majors	Number
CISO in TMT with IT background	information systems, management information systems, computer information systems, computer science, information technology, information assurance, computer networks, information security, information management, information & computer science, security management, technology management, systems analysis	138
CISO in TMT with business background	finance, accounting, marketing, risk management, international business, human resources, business administration, business studies, management, economics, Master of Business Administration (MBA), computer information systems, information systems, management information systems	153
CISO in TMT with STEM background	engineering, physics, computer science, mathematics, biology, astronomy	204
CISO in TMT with legal studies or criminology background	law, legal, criminal justice, juris doctorate, JD related degree	40
CISO in TMT with other backgrounds	including but not limited to history, zoology, sociology	22
CISO in TMT with unclear background	only has degree information but no major information	6
CISO in TMT without specifying background	NA	39
CISO in TMT without a LinkedIn account	NA	50

Note: Total number of CISOs: 418

Variables	(1) Business	(2) IT	(3) Legal studies or criminology	(4) STEM
CISOTMT				
Without CISOTMT	-0.030	-0.030	-0.084**	-0.074
	(0.048)	(0.043)	(0.040)	(0.046)
CISOTMT With Specific Background	0.121*	0.133*	-0.040	0.012
	(0.069)	(0.071)	(0.123)	(0.068)
CISOTMT Without Specific Background	Baseline	Baseline	Baseline	Baseline
FirmSize	0.084***	0.085***	0.084***	0.084***
	(0.018)	(0.018)	(0.018)	(0.018)
Profitability	-0.085	-0.086	-0.087	-0.087
	(0.061)	(0.062)	(0.061)	(0.062)
Leverage	0.151***	0.151***	0.151***	0.151***
	(0.028)	(0.028)	(0.028)	(0.028)
AssetTangibility	0.239**	0.239**	0.241**	0.240**
	(0.094)	(0.094)	(0.094)	(0.094)
CapitalExpenditure	-0.045	-0.045	-0.046	-0.046
	(0.090)	(0.090)	(0.090)	(0.090)
R&DExpenditure	2.202***	2.207***	2.171**	2.175**
	(0.849)	(0.850)	(0.849)	(0.849)
TechOfficer	0.042***	0.041***	0.042***	0.042***
	(0.015)	(0.015)	(0.015)	(0.015)
CROPresence	0.004	0.006	0.006	0.006
	(0.024)	(0.024)	(0.024)	(0.024)
CInnOPresence	-0.003	-0.002	-0.002	-0.002
	(0.036)	(0.036)	(0.036)	(0.036)
FirmAge	0.167***	0.167***	0.167***	0.167***
	(0.035)	(0.035)	(0.035)	(0.035)
GrowthOpportunity	0.000**	0.000**	0.000**	0.000**
	(0.000)	(0.000)	(0.000)	(0.000)
IndustryTurbulence	0.256***	0.251***	0.251***	0.251***
	(0.092)	(0.093)	(0.093)	(0.093)
MarketConcentration	-0.140	-0.140	-0.141	-0.142
	(0.219)	(0.217)	(0.218)	(0.219)
IndustryGrowth	0.083	0.076	0.079	0.079
	(0.077)	(0.076)	(0.077)	(0.077)
Firm Fixed Effects	Yes	Yes	Yes	Yes
Quarter Fixed Effects	Yes	Yes	Yes	Yes
R^2	0.107	0.107	0.106	0.106

Notes: Number of observations: 70650; Significance levels: *p < 0.1, **p < 0.05, ***p < 0.01; Cluster standard errors are in parentheses.

APPENDIX F

Results of Additional Robustness Checks

Alternative Definitions of Industry Boundaries

Variables	**(1)**	**(2)**
	4 digits	**5 digits**
SpecialistCISOTMT	0.169*** (0.064)	0.159*** (0.061)
GeneralistCISOTMT	0.110** (0.046)	0.109** (0.053)
IndustryTurbulence	0.081 (0.050)	0.075** (0.036)
SpecialistCISOTMT × *IndustryTurbulence*	-0.176 (0.363)	-0.099 (0.308)
GeneralistCISOTMT × *IndustryTurbulence*	**-0.507** (0.240)**	**-0.532** (0.230)**
FirmSize	0.085*** (0.018)	0.085*** (0.018)
Profitability	-0.087 (0.061)	-0.087 (0.061)
Leverage	0.151*** (0.030)	0.150*** (0.030)
AssetTangibility	0.236** (0.094)	0.234** (0.094)
Capital expenditure	-0.048 (0.091)	-0.048 (0.091)
R&DExpenditure	2.190** (0.849)	2.195*** (0.850)
TechOfficer	0.042*** (0.015)	0.043*** (0.015)
CROPresence	0.006 (0.024)	0.006 (0.024)
CInnOPresence	-0.005 (0.036)	-0.004 (0.036)
FirmAge	0.166*** (0.035)	0.167*** (0.035)
GrowthOpportunity	0.000** (0.000)	0.000** (0.000)
MarketConcentration	-0.133 (0.218)	-0.132 (0.218)
IndustryGrowth	0.070 (0.076)	0.072 (0.076)
Firm Fixed Effects	Yes	Yes
Quarter Fixed Effects	Yes	Yes
R^2	0.107	0.107

Notes: Number of observations: 70650; Significance levels: *$p < 0.1$, **$p < 0.05$, ***$p < 0.01$; Cluster standard errors are in parentheses.

Moderating Effects of Industry Experience Using Median as Threshold

	(1)	(2)
Variables	**Innovation**	**Innovation**
WithoutCISOTMT	Baseline	Baseline
SpecialistCISOTMT	0.095* (0.052)	0.137** (0.066)
GeneralistCISOTMT	0.066 (0.044)	0.197*** (0.065)
SpecialistCISOTMT × *IndustryTurbulence*		-0.341 (0.496)
GeneralistCISOTMT × *IndustryTurbulence*		-1.018** (0.448)
IndustryTurbulence	0.253*** (0.093)	0.315*** (0.100)
FirmSize	0.084*** (0.018)	0.085*** (0.018)
Profitability	-0.087 (0.061)	-0.085 (0.061)
Leverage	0.151*** (0.028)	0.153*** (0.028)
AssetTangibility	0.241** (0.094)	0.238** (0.094)
CapitalExpenditure	-0.047 (0.090)	-0.040 (0.090)
R&DExpenditure	2.172** (0.849)	2.171** (0.848)
TechOfficer	0.042*** (0.015)	0.042*** (0.015)
CROPresence	0.006 (0.024)	0.005 (0.024)
CInnOPresence	-0.002 (0.036)	-0.004 (0.036)
FirmAge	0.167*** (0.035)	0.168*** (0.035)
GrowthOpportunity	0.000** (0.000)	0.000** (0.000)
MarketConcentration	-0.145 (0.218)	-0.155 (0.218)
IndustryGrowth	0.079(0.077)	0.075 (0.077)
Firm Fixed Effects	Yes	Yes
Quarter Fixed Effects	Yes	Yes
R^2	0.106	0.107

Notes: Number of observations: 70650; Significance levels: *$p < 0.1$, **$p < 0.05$, ***$p < 0.01$; Cluster standard errors are in parentheses.

APPENDIX G

Cybersecurity-Related 8-K Keywords for SEC Data Breach

Categorization	List of Keywords
Full Descriptions of Keywords	"cyber-attack", "cyber attack", "cybersecurity incident", "cyber threat", "cyberattack", "cyber-intrusion", "cyber incident", "ransomware attack", "ransomware incident", "unauthorized activity", "unusual activity", "illegal intrusion", "suspicious activity", "theft", "unauthorized access", "unauthorized breach", "unauthorized", "criminal fraud", "criminal intrusion", "fraud perpetrated", "data incident", "security incident", "security issue", "security update", "security breach", "malware incident", "malware,"
Abbreviation of Keywords	"cyber", "suspicious", "intrusion", "ransomware", "attack", "unauthorized", "theft", "criminal", "fraud", "malware", "security breach", "security issue", "data breach", "unusual activity"

Row one summarizes keywords directly extracted from 8-K filings. Row two shows extracted key parts of the keywords for further analysis as a completeness check. The keyword abbreviations generated more results, but each keyword was manually verified by the authors to ensure it was a data breach notification.

APPENDIX H

Coding of IT Executive Positions and Examples

Keywords	Examples/Full Name
cio	Full name: chief information officer
cto	Full name: chief technology officer
cdo	Full name: chief data officer/ chief digital officer
ciso	Full name: chief information security officer
data	chief data analytics officer
digit	chief digital officer
secur	chief security officer
info	chief information officer
tech	chief technology officer
privacy	data privacy officer
mobile	chief mobile officer
software	chief software technology officer
system	chief systems officer
analytics	division chief analytics officer
network	chief network officer
program	chief programming executive
app	chief application development officer
artificial	chief artificial intelligence officer
architecture	systems architecture

APPENDIX I

Correlation Table of Compensation and Data Breach Disclosure Paper

Variables	1	2	3	4	5	6	7	8	9	10
1. Disclosed	1.00									
2. IT Compensation	-0.00	1.00								
3. Non-IT Compensation	-0.06*	0.33*	1.00							
4. Board Cybersecurity Intensity	-0.01	0.03*	0.07*	1.00						
5. Firm Size	-0.02*	0.14*	0.36*	0.06*	1.00					
6. ROA	-0.01	0.06*	0.15*	0.01	0.16*	1.00				
7. Tobin's q	0.01	0.03*	-0.00	-0.02*	-0.21*	-0.23*	1.00			
8. Leverage	0.00	-0.00	0.00	0.00	0.04*	-0.00	-0.01	1.00		
9. Asset Tangibility	-0.00	-0.05*	-0.01	-0.03*	-0.10*	0.03*	-0.00	-0.01	1.00	
10. MBA	0.00	0.01	0.01	-0.00	-0.02*	0.09*	-0.10*	-0.00	-0.00	1.00
11. MBE	0.00	0.00	0.02*	0.00	0.01	0.02*	0.00	0.02*	0.00	0.00
12. R&D	0.01	0.06*	-0.10*	-0.02*	-0.24*	-0.24*	0.29*	-0.00	-0.11*	-0.01
13. EPR	-0.00	-0.00	-0.01	0.00	0.02*	0.19*	-0.00	0.00	-0.01	0.01
14. CAPEX	-0.00	-0.01	-0.01	0.00	-0.12*	-0.00	0.10*	-0.02*	0.34*	0.02*
15. Age	0.00	-0.08*	0.00	-0.00	0.16*	-0.01	-0.09*	0.00	0.07*	0.01
16. Gender	-0.01	-0.00	-0.01	-0.02*	0.02*	-0.02*	-0.02*	0.01	-0.03*	0.01
17. Breach Severity	-0.01	0.03*	0.14*	-0.01	0.03*	0.04*	0.03*	-0.02*	-0.02*	0.02*
18. Breach Public Attention	0.03*	-0.02*	0.06*	-0.04*	0.07*	0.01	0.02*	-0.00	-0.06*	0.01
19. Board Dependent Ratio	-0.00	-0.01	-0.09*	-0.01	-0.09*	-0.04*	0.10*	-0.00	-0.02*	-0.05*
20. Industry Type	0.01	-0.01	-0.06*	0.03*	-0.00	0.03*	0.05*	0.00	-0.25*	-0.00

Variables	11	12	13	14	15	16	17	18	19	20
11. MBE	1.00									
12. R&D	0.01	1.00								
13. EPR	0.01	-0.01	1.00							
14. CAPEX	-0.02*	0.04*	-0.00	1.00						
15. Age	0.01	-0.08*	0.00	-0.04*	1.00					

16. Gender	0.00	0.01	0.00	-0.03*	0.08*	1.00				
17. Breach Severity	0.00	-0.04*	-0.00	0.01	0.02*	0.00	1.00			
18. Breach Public Attention	0.02*	-0.02*	0.00	0.00	0.01	0.03*	0.05*	1.00		
19. Board Dependent Ratio	0.00	0.08*	0.00	0.03*	-0.03*	-0.01	-0.04*	-0.00	1.00	
20. Industry Type	-0.02*	-0.10*	-0.01	-0.04*	-0.13*	0.01	0.04*	0.05*	0.02*	1.00

Note: Number of observations: 17020; *$p < 0.05$.

APPENDIX J

Correlation Table of Reporting Structure Paper

Variables	1	2	3	4	5	6	7	8	9	10
1. *ProspectivePerformance*										
2. *RetrospectivePerformance*	0.09*									
3. *DigitalTransformation*	0.06*	0.07*								
4. *SecurityAwareness*	-0.01	0.01	0.05*							
5. *CDOWithinGroupReporting*	0.01	0.05*	-0.00	0.00						
6. *CDOAcrossGroupReporting*	0.01	0.06*	0.06*	-0.00	-0.02*					
7. *CISOWithinGroupReporting*	-0.03*	0.12*	0.01	0.01	0.17*	0.13*				
8. *CISOAcrossGroupReporting*	-0.03*	0.11*	0.03*	0.03*	-0.01	0.09*	-0.02*			
9. *FirmSize*	-0.12*	0.55*	0.03*	0.03*	0.11*	0.09*	0.17*	0.16*		
10. *FirmAge*	-0.04*	0.21*	-0.01	0.02*	0.02*	0.01	0.08*	0.05*	0.34*	
11. *BookLeverage*	0.08*	0.10*	0.01	-0.02	-0.02	-0.00	0.02*	-0.02*	0.11*	-0.03*
12. *IndustryTurbulence*	0.02*	0.03*	0.02*	-0.02*	0.01	0.01	0.00	-0.04*	-0.10*	-0.10*
13. *IndustryGrowth*	-0.05*	-0.04*	-0.02*	0.04*	-0.01	-0.01	0.04*	0.04*	0.08*	-0.02*
14. *MarketConcentration*	-0.04*	0.04*	0.01	-0.03*	0.03*	0.05*	0.06*	0.02*	-0.04*	-0.02
15. *FemaleRatio*	-0.01	-0.02	0.04*	-0.05*	0.02*	0.01	0.00	-0.05*	-0.05*	-0.00
16. *AverageAge*	0.00	0.02*	-0.02	-0.12*	0.02*	-0.07*	-0.03*	-0.06*	-0.05*	0.01
17. *TotalTMT*	0.05*	0.25*	0.07*	0.05*	0.25*	0.35*	0.36*	0.29*	0.34*	0.11*
18. *AvgSub*	0.00	0.25*	0.03*	0.02*	0.13*	0.16*	0.17*	0.15*	0.36*	0.21*
19. *MoreCISOPeer*	-0.03*	0.08*	0.01	0.02*	0.11*	0.09*	0.32*	0.50*	0.14*	0.05*
20. *MoreCDOPeer*	0.02	0.07*	0.03*	-0.01	0.33*	0.54*	0.14*	0.04*	0.10*	0.01
Variables	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**
12. *IndustryTurbulence*	-0.05*									
13. *IndustryGrowth*	0.11*	-0.35*								
14. *MarketConcentration*	0.06*	0.21*	-0.02*							
15. *FemaleRatio*	-0.06*	0.08*	-0.16*	0.00						
16. *AverageAge*	-0.10*	0.14*	-0.27*	-0.04*	0.35*					
17. *TotalTMT*	0.03*	-0.02	0.04*	0.06*	-0.01	-0.08*				
18. *AvgSub*	0.07*	-0.07*	0.09*	0.03*	-0.00	-0.06*	0.43*			

19. *MoreCISOPeer*	-0.01	-0.01	0.04*	0.01	0.00	-0.04*	0.27*	0.15*	
20. *MoreCDOPeer*	-0.02	0.04*	-0.00	0.08*	0.04*	-0.02*	0.28*	0.15*	0.17*

Notes: Number of observations: 12979; $^*p < 0.05$.