

THREE ESSAYS ON THE ECONOMICS OF INFORMATION SECURITY

A Dissertation
Submitted to
the Temple University Graduate Board

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

by
Leting Zhang
Diploma Date August 2022

Examining Committee Members:

Dr. Sunil Wattal, Advisory Chair, Department of MIS

Dr. Taha Havakhor, Department of MIS

Dr. Subodha Kumar, Department of Statistics, Operations, and Data Science

Dr. Anthony Vance, Department of Business Information Technology, Virginia Tech

Dr. Oleg Rytchkov, External Reader, Department of Finance

©
Copyright
2022

by

Leting Zhang

All Rights Reserved

ABSTRACT

In recent years, information security has been gaining increasing public attention and has become a high priority for organizations across various industries. Despite the substantial investment in improving security posture, cyber risks continue to escalate as digital transformations are growing rapidly, and new areas of cyber-vulnerability are exposed and exploited. Thus, a critical question for managers, stakeholders, and policymakers is: How to strategically ensure the security of digital assets? To explore the question, my dissertation explores and advances three critical themes in the economics of the information security field. These themes include: 1) unraveling antecedents of risks, 2) determining the optimal level of investment in cybersecurity, and 3) investigating how cybersecurity affects market dynamics. Essay 1 is motivated by security concerns in sharing data across organizations and empirically evaluates the impact of joining a Health Information Exchange (HIE) initiative on a hospital's data breach risks and corresponding mechanisms. Essay 2 uses a game theoretical model to investigate how to design a cost-effective crowdsourcing solution to help organizations leverage crowds' wisdom in vulnerability management. Essay 3 examines the role of peer cyber incidents in information asymmetry issues in the financial market and analyze how peer data breaches affect the quality of a firm's cyber risk disclosure in its financial report. The dissertation sheds light on three crucial factors in information security management: information systems interdependency, innovated cybersecurity solutions, and cyber information asymmetry.

ACKNOWLEDGMENTS

My Ph.D. journey is a wonderful and challenging adventure. There are so many people I would like to thank.

First, I would like to express my deep gratitude to my advisor Dr. Sunil Wattal for his guidance, time, and patience. Since I entered the Ph.D. program, Sunil helped me navigate graduate schools and gave me many advice about doing high-quality research. He encouraged me to explore different topics and submit manuscripts. Furthermore, he kept setting high standards for details in research, pushing me to sharpen my logical thinking and improve my writing skills. It has been my genuine pleasure to have him as an advisor and to have the opportunity of working with him.

I would like to extend my gratitude to my dissertation committee members, Dr. Subodha Kumar, Dr. Anthony Vance, Dr. Taha Havakhor, and Dr. Oleg Rytchkov, for their unparalleled support of my research and mentorship in my doctoral study. I benefited substantially from working with Subodha on analytical modeling research. He instructed me to use different optimization methods which became powerful tools in my research skillset. I want to thank Tony as a kind and helpful mentor in the cybersecurity area. In our many discussions, I can always learn new and important trends in the area from his input. I'm also very fortunate to work with Taha. He gave me many insightful suggestions for doing empirical works and helped me substantially in job searching. I really appreciate Oleg's excellent econometrics courses and his insightful comments on my research.

I want to thank other faculty members who have helped me. I thank Dr. Emre Demirezen who patiently guide me in writing analytical modeling papers. I benefited a lot from Prof. Christina M. Owings's lecture on communication and writing. I am thankful to valuable suggestions from Drs. David Schuff, Munir Mandviwalla, Min-Seok Pang, Jason Thatcher, Sezgin Ayabakan, and Jing Gong. I am also grateful to my master thesis advisor Dr. Qihong Wang for encouraging me to pursue a PhD.

Without her support and advice, I may not apply for a PhD and would never finish the dissertation.

My PhD cohorts gave me enormous supports. I especially thank my peer Xi Wu who is also my genuine friend. The times that we have spent together discussing research and attending conferences are invaluable. I also appreciate the critics and advice from senior PhD friends, Zuyin (Alvin) Zheng, Zhi (Aaron) Cheng, Shuting (Ada) Wang, Zhe Deng, Xue Guo, and Samayita Guha. I would like to acknowledge other PhD friends, Yiwen Gao, Youngjin Kwon, Hyeonsik Shin, Guohou Shan, Dongwook Chun, Meixian Wang, Ziyi Zhao, and Kanghyun Cho.

My sincere thanks also go to my best friends Mengze Chen, Chanjuan Huang, Tingting Huang, and Rihuan Huang. They always back me up during my ups and downs. Without their precious support, I would not have come this far.

Last but not least, I want to thank people who have significant influence on my life. I cannot thank my partner Xinyuan enough for encouraging me to pursue academic excellence. I'm deeply indebted to my parents Yanjun Zhang and Haiyan Luo for their endless love. No matter what, they always believe me and support me unconditionally. I also appreciate my admirable grandparents for taking care of me, and for teaching me to treat others kindly and be an upright person. I'm extremely grateful to Weiyu Luo, my cousin, for his wisdom, courage, and kindness. I will always remember our deep conversations about freedom and equality. He will always be a hero in my heart.

TABLE OF CONTENTS

	Page
ABSTRACT	iii
ACKNOWLEDGMENTS	iv
LIST OF TABLES	x
LIST OF FIGURES	xii
 CHAPTER	
1 INTRODUCTION	1
2 DOES SHARING MAKE MY DATA MORE INSECURE? AN EMPIRICAL STUDY ON HEALTH INFORMATION EXCHANGE AND DATA BREACHES	6
2.1 Introduction	6
2.2 Literature Review	10
2.2.1 Interdependent Risks	10
2.2.2 Inter-organizational Systems and Governance	11
2.2.3 Organizational IT Practices and Information Security	12
2.3 HIEs and Data Security	13
2.3.1 Data Breach Risks in Joining an HIE	14
2.3.2 HIE’s Data Security Governance	15
2.4 Theoretical Framework	16
2.4.1 A Baseline Case	17
2.4.2 A Case with Information Exchange	18
2.4.3 Comparison of the Two Cases	20
2.5 Data Description	22
2.5.1 Outcome and Treatment Variables	23
2.5.2 Control Variables	24

	Page
2.6	Empirical Specifications 27
	2.6.1 Difference in Differences 27
	2.6.2 Matching Strategies 28
2.7	Analyses 29
	2.7.1 IT Security Investment 30
	2.7.2 Data Breach Outcomes 31
	2.7.3 IT Security Capability 32
	2.7.4 HIE Security Laws 37
2.8	Robustness Checks 38
	2.8.1 Endogeneity and Identification Strategies 38
	2.8.2 Relative Time Models 41
	2.8.3 Instrumental Variables 42
	2.8.4 Time-varying Treatment Effects 45
	2.8.5 Other Sensitivity Tests 47
2.9	Additional Analyses 47
	2.9.1 Breaches of Different Locations 47
	2.9.2 Breaches of Different Threat Actors 49
2.10	Discussion 50
	2.10.1 Main Findings 50
	2.10.2 Implications for Research 51
	2.10.3 Implications for Practice 52
	2.10.4 Limitations and Future Directions 54
3	HOW TO MAKE MY BUG BOUNTY COST-EFFECTIVE? A GAME- THEORETICAL MODEL 56
	3.1 Introduction 57
	3.1.1 Motivation 58
	3.1.2 Research Questions and Contributions 62
	3.1.3 Literature Review 64
	3.2 Model 67

	Page
3.2.1 Security Researchers	68
3.2.2 Characteristics of the Organization	71
3.2.3 Sequence of the Game	76
3.3 Solutions	76
3.4 Results and Managerial Insights	78
3.4.1 How Do the Organization’s Characteristics Impact the Bounty?	78
3.4.2 How Do Security Researchers Impact the Bounty and the Total Cost of the BBP?	81
3.4.3 How Does Legal Protection Impact the Bounty and To- tal Cost?	90
3.5 Extensions	94
3.5.1 Strategic Hacker	94
3.5.2 Endogenize Organization’s Security Posture	95
3.5.3 Multiple Vulnerabilities	95
3.6 Discussion and Conclusion	96
3.6.1 Practical Implications for Bounty Design	96
3.6.2 Future Research Opportunities	98
4 PEER DATA BREACHES AND CYBER RISK DISCLOSURE QUALITY: EVIDENCE FROM U.S. PUBLIC FIRMS	99
4.1 Introduction	99
4.2 Literature Review	102
4.2.1 Impacts of IT Security Incidents	103
4.2.2 Industry Peers	104
4.2.3 Voluntary Disclosure Incentives	105
4.3 Background and Conceptual Model	106
4.4 Data Description	108
4.4.1 Cyber Risks Disclosure	109
4.4.2 Measure Cyber Risks Disclosure Quality	112
4.4.3 Industry Peers’ Data Breaches	114

	Page
4.5	Main Empirical Analyses 116
4.6	Robustness Analyses 118
4.6.1	Main Effect: Instrumental Variables 118
4.6.2	Main Effect: Industry and State Specific Trends . . . 121
4.6.3	Main Effect: Alternative Measurements 121
4.7	Heterogeneity Analyses 124
4.7.1	Internal Risks Assessment 124
4.7.2	Public Attention 126
4.8	Additional Analyses 128
4.8.1	Cyber Risks Disclosure Length 128
4.8.2	Cybersecurity Investment 129
4.8.3	Analyst Coverage 129
4.9	Summary and Discussion 131
4.9.1	Conclusion and Contribution 131
4.9.2	Limitations and Future Directions 132
5	SUMMARY AND FUTURE RESEARCH 133
	APPENDICES 136
A	APPENDIX - STUDY 1 136
B	APPENDIX - STUDY 2 139
B.1	Main Model 139
B.2	Extension 1: Strategic Hacker 143
B.3	Extension 2: Endogenize Security Posture 147
B.4	Extension 3: Multiple Vulnerabilities 150
C	APPENDIX - STUDY 3 154
	REFERENCES CITED 156

LIST OF TABLES

Table	Page
2.1 A Summary of Lemmas	22
2.2 Summary Statistics	26
2.3 Propensity Scores Matching – Descriptive Analyses	29
2.4 The Impact of Joining HIE on Hospital’s IT Security Investment	31
2.5 The Impact of Joining HIE on Hospital’s Data Breaches	33
2.6 Heterogeneity Analysis: Hospital’s IT Security Capability	36
2.7 Heterogeneity Analysis: HIE Security Law	38
2.8 Summary of Robustness Tests	40
2.9 Relative-time Model	42
2.10 Instrument Variables – 2SLS Estimations	45
2.11 Bacon Decomposition Results	47
2.12 Definitions of Breach Locations	48
2.13 Different Types of Breaches: Locations	48
2.14 Different Types of Breaches: Threat Actors	50
3.1 List of Key Parameters and Variables	67
4.1 Summary Statistics	109
4.2 The Impact of Peer Breaches on Cyber Risk Disclosure Quality	117
4.3 Instrument Variables - 2SLS Estimations	120
4.4 Industry and State Specific Trends	122
4.5 Alternative Measurements	123
4.6 Heterogeneity Analysis: Susceptibility to Data Breaches Risks	125
4.7 Heterogeneity Analysis: Public Attention	128
4.8 Additional Analyses	130
A.1 Correlation Matrix	136
A.2 Robustness Check: State-year Specific Trends	137

Table	Page
A.3 Robustness Check: Non-linear Models	138
C.1 Correlation Matrix	154
C.2 Cybersecurity Keywords Used to Extract Cyber Risk Disclosure (CRD)	155
C.3 Cybersecurtiy Applications in CITDB	155

LIST OF FIGURES

Figure	Page
1.1 Dissertation Framework	3
2.1 HIE Participation Rates	24
2.2 The Marginal Effect of HIE on A Hospital's Data Breach Likelihood by its IT Security Capability	36
2.3 Bacon Decomposition Results	46
3.1 The Marginal Effect of an Additional Security Researcher on the Optimal Bounty as a Function of Productivity Heterogeneity $\frac{\bar{a}}{a}$ and PR Effect θ	84
3.2 The Marginal Effect of an Additional Security Researchers on the Equilibrium Total Cost as a Function of Productivity Heterogeneity $\frac{\bar{a}}{a}$ and PR Effect θ	89
4.1 Cyber Risk Disclosure in Target's 2011 10-K	110
4.2 Cyber Risk Disclosure Trends - Proportion of Public Firms	111
4.3 Cyber Risk Disclosure Trends - Lengths	111
4.4 The Processes of Measuring Cyber Risk Disclosure Similarities	113
4.5 The Wordcloud of Processed Cyber Risks Disclosure Documents based on TF-IDF Weights	114
4.6 Public Firms' Data Breaches from 2011 to 2017	115
4.7 Industries and Data Breaches	115
4.8 Google Trends - Data Breaches	127

CHAPTER 1

INTRODUCTION

Information security is becoming a greater priority for organizations in the digital age. The increasing dependency on software and IT systems leads to higher uncertainties and cyber risks. The challenge is especially salient considering that information security incidents incur substantial economic losses to businesses and society. High-profile incidents such as the 2017 Equifax data breaches and the 2020 SolarWinds hacking received wide public attention because of the large scope of the damage. For another thing, stringent regulations across the globe are taking effect. Data Breach Notification Laws and California Consumer Privacy Act (CCPA) in the US, General Data Protection Regulation (GDPR) in the EU, and Personal Information Protection Law (PIPL) in China impose detailed data governance requirements and penalties for non-compliance. Therefore, it is imperative for organizations across industries to continue elevating information security as a strategic issue.

Information Systems (IS) literature extensively investigates information security in organizations from economic and managerial views. According to the literature, I identify three main themes in this field, namely *antecedents of risks*, *optimal investment*, and *market dynamics*. First, *antecedents of risks* studies focus on factors that exacerbate or mitigate information security risks. Individual-level studies examine what leads to information security policy (ISP) compliance or violation by drawing on theories from criminology and psychology (Siponen and Vance 2010, Vance et al. 2018, Wang et al. 2015). Organization-level studies evaluate security implications of practices that are internal or external to organizations, including enterprise technologies adoptions (Kim and Kwon 2019), institutional factors (Angst et al. 2017), subcultures (Sarkar et al. 2020), corporate social responsibility (D'Arcy et al. 2020), and corporate governance (Wang et al. 2013).

Second, *optimal investment* studies shed light on how to allocate resources or design markets to improve security performance. Besides examining general information security investment in organizations (Gordon and Loeb 2002, Kwon and Johnson 2014), an increasing number of studies examine the benefits and costs of specific security operations and policies. For instance, those studies investigate vulnerability disclosures policy (Arora et al. 2008, Ransbotham and Mitra 2009, Sen et al. 2019), security monitoring (Ji et al. 2016), mandatory standards (Lee et al. 2016), contracts in outsourcing (Cezar et al. 2014), and security patching (August et al. 2019).

Third, *market dynamics* studies aim to understand how market participants' behaviors and outcomes are affected by information security related events such as data breaches, cyber risk disclosures, and IT security investment. Literature in this theme explores the economic impacts of software vulnerability announcements (Telang and Wattal 2007), market responses to cyber risk disclosures (Gordon et al. 2010, Florakis et al. 2020, Havakhor et al. 2020), and how information security characteristics shape market competition (Dey et al. 2014) and segmentation (August et al. 2014).

Building on previous research, my dissertation aims to expand and advance the literature by analyzing one key feature in the above themes: *interdependence, innovation, and information asymmetry*. These features are increasingly prevalent but have not been adequately explored before. Building on information systems and economic theories, I focus on the role of institutions in IT interdependence among organizations, the optimal decision in innovative crowdsourcing cybersecurity solutions, and the incentives of public firms in disclosing cyber risks. Figure 1.1 presents the framework of the dissertation. Next, I briefly introduce the three essays in my dissertation.

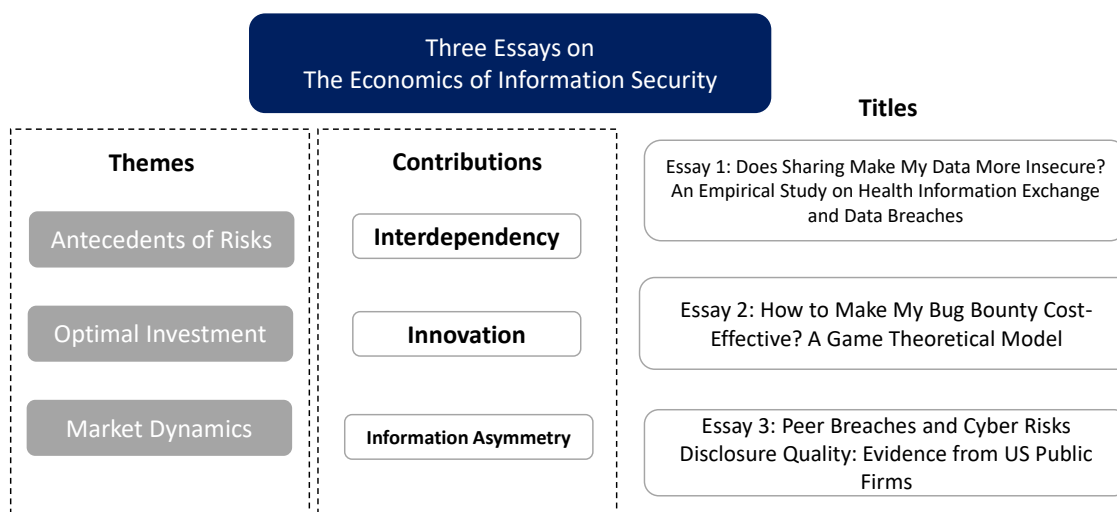


Figure 1.1. Dissertation Framework

The first essay examines how adopting inter-organizational systems impacts individual organizations' data breach risks. By analyzing the IT risks and governance that IT system "interdependence" introduce, it fills an important gap in the literature on the antecedents of cyber risks. The study focuses on electronic Health Information Exchange (HIE) in the healthcare industry. As an inter-organizational information system, HIE facilitates healthcare data sharing among healthcare providers. Therefore, HIE has long been regarded as helpful in improving operational efficiency and service quality. Although the public concerns regarding data breach risks have increased as more hospitals adopt HIE and exchange their data through HIE systems, there is no study empirically examine the impact. To fill the gap, my first essay tries to answer the question: *How does joining an HIE affect a hospital's data breach risks?* To examine the question, I use a six-year panel data on hospitals' HIE participation statuses, institutional characteristics, IT characteristics, and data breach

incidents from multiple sources. The results show that the likelihood that a hospital experiences data breaches decreases by 1.7 percentage points (34% reduction) after joining an HIE. I further show that the magnitude of the effect is larger when HIE member hospitals have greater IT security capability, or after HIE security laws were enacted. Additionally, the likelihood of experiencing IT system breaches and hacking incidents significantly decrease after a hospital joins an HIE. However, there are no significant changes in the likelihoods of physical breaches and internal breaches. This paper contributes to the information systems literature by studying the impact of IOS adoption on organizational data breaches. It also sheds light on the mechanisms of data security governance in the IOS context.

The second essay investigates the incentive design in a cybersecurity solution - Bug Bounty Program. It contributes to the stream of literature on the optimal investment in cybersecurity by analyzing the potential costs and benefits of a bug bounty program that facilitates “innovation” in vulnerability discoveries. In practice, many organizations leverage bug bounty programs to attract external security researchers to search for new vulnerabilities in their IT systems. However, one key question for the organizations is: *How to design a bug bounty program and improve its cost-effectiveness?* To shed light on this question, I use a game-theoretical model to examine several related research questions where I consider the characteristics of (i) the organization’s security posture and patching complexity, (ii) security researchers’ efficiency and number, and (iii) the level of legal protection for security researchers. The findings reveal that organizations need to be strategic in designing bounties when their patching complexity is high. However, organizational security postures can substitute for bounties. Furthermore, having a more capable or a larger number of security researchers may not necessarily imply an increased bounty and lower total costs. A bounty’s public relations effect plays a critical role in deciding the changes. Lastly, when there is increased legal protection for security researchers, an organization may increase the bounty size and experience lower total costs. This study provides several insights to security professionals, organizations, and policymakers in designing effective bug bounty programs.

The third essay analyzes how the quality of a firm's cyber risk disclosure is affected by its peer firms' data breaches. It sheds light on the impact of realized cyber incidents on "information asymmetry" issues in the financial market and contributes to the literature on how cyber incidents affect market dynamics. Public firms' cyber risks disclosures are becoming increasingly critical and more scrutinized. However, when there are more mandatory disclosures about security incidents, how the dynamics affect voluntary disclosures are seldom examined. In this study, I explore a specific question: *How do peer breaches affect a firm's voluntary cyber risks disclosure (CRD) quality?* To answer this question, I first construct a proxy for CRD quality by leveraging rich textual characteristics in public firms' annual filings. Next, I compile an innovative dataset from multiple resources, and the dataset covers firms' financial performance, auditing information, and IT characteristics. The findings suggest that firms strategically lower the CRD quality after peer breaches. Furthermore, the CRD quality decreases at a larger magnitude when firms have less IT security protection or have more sites. The public attention to cyber risks also exacerbates the decrease in CRD quality. Interestingly, the reduction in CRD quality is lower on firms has high cybersecurity investment and analyst coverage. To address endogeneity concerns, I leverage several identification strategies, and the results are robust to different specifications, alternative measurements, and 2SLS estimations with instruments. This study complements the economics of information security and corporate disclosures. In addition, it provides practical implications for investors and policymakers in terms of understanding firms' incentives in disclosing cyber risks.

To summarize, the three essays examine information security in different contexts where new challenges and opportunities regarding security protection arise. Furthermore, they quantify the security related outcomes and shed light on related mechanisms. These essays expand literature and provide managerial insights for stakeholders, managers, and policymakers.

CHAPTER 2

DOES SHARING MAKE MY DATA MORE INSECURE? AN EMPIRICAL STUDY ON HEALTH INFORMATION EXCHANGE AND DATA BREACHES

Abstract

This paper examines the information security implications of participating in inter-organizational systems (IOS) in the context of the healthcare industry. As more hospitals share their data through electronic Health Information Exchange (HIE), a type of IOS, public concern has grown regarding the security of healthcare data. In this study, we examine the impact of joining an HIE on hospitals' data breach risks, by compiling a panel dataset of more than 3000 hospitals from 2010 to 2015. Using a difference-in-differences design, we find that the likelihood that a hospital experiences data breaches decreases by 1.7 percentage points (43% reduction) after joining an HIE. We further show that the magnitude of the effect is larger when HIE member hospitals have greater IT security capability, or after HIE security laws were enacted. Additionally, the likelihoods of experiencing IT system breaches and hacking incidents significantly decrease after a hospital joins an HIE. However, there are no significant changes in the likelihoods of physical breaches and internal breaches. We discuss the implications for research and practice.

2.1 Introduction

The security of health data has become the subject of intense interest among scholars and hospital administrators alike (Esmaeilzadeh and Mirzaei 2019). A 2021 report (IBM 2021) shows that security breaches in the healthcare industry cost an average of \$9.23 million per incident, the highest of any industry in terms of cost. These

breaches not only affect healthcare organizations, which incur substantial expenses in breach remediation and damage to businesses; they also impact individuals, who face potential financial and medical identity theft (Greig 2022). Many practitioners and scholars attribute hospitals' high data breach risk to digitalization initiatives (Hoffman and Podgurski 2009, Kim and Kwon 2019, Perlroth 2011, Seh et al. 2020, Sittig and Singh 2011). As more hospitals electronically share medical information across organizational boundaries through Health Information Exchange (HIE), data security concerns have become more pronounced.

HIE is one of the most important initiatives in healthcare's digital transformation. It promotes health data exchange and interoperability standards, facilitating efficient sharing of electronic patient information between unaffiliated health systems. The acronym "HIE" can refer to either a network that healthcare stakeholders can join, or an IT application that allows a hospital to exchange electronic information with outside organizations. To clarify the definitions, we use *HIE* to stand for *HIE network* and use *HIE app* to stand for *HIE application*.¹ Sharing patient information via an HIE can generate benefits to the healthcare sector, including improving the quality of care, reducing duplicate costs, and lowering Medicare expenditures, among others (Adjerid et al. 2018, Atasoy et al. 2017, Ayabakan et al. 2017). Therefore, it draws substantial attention from healthcare stakeholders. In 2009, the passage of the HITECH Act in the United States promoted the adoption of electronic health records (EHR) and HIE by healthcare providers through monetary incentives (Burde 2011). By 2018, about 70% of acute care hospitals were connected to more than one HIE with nationwide scope (Monica 2018). Nevertheless, electronic data sharing may introduce breach risks among HIE participants.

For healthcare organizations, joining an HIE promises new useful IT functionalities, which can also cause technological disruptions and increase IT security risks. An HIE app is a type of inter-organizational system (IOS) that links different participants; this renders key components of risk, such as threats and vulnerabilities, no

¹In this paper, "a hospital joins an HIE" and "a hospital adopts an HIE app" have exactly the same meaning.

longer isolated to any individual participant (Huang et al. 2014). For instance, on July 13, 2016, Codman Square Health Center in Massachusetts was notified of a data breach incident wherein an unauthorized person obtained access to New England Healthcare Exchange Network. The incident led to a data breach of 140 Codman patients' information along with that of more than 4,000 others in the HIE (McGee 2016). Several healthcare experts have voiced concerns about the security implications of joining HIEs.² A survey by the Ponemon Institute found that more than 72 percent of healthcare providers have somewhat or no confidence in sharing patient data on HIEs.³

However, because of the interdependence among organizations, data governance is also designed and used in HIEs to coordinate data sharing (Adjerid et al. 2018; McGowan et al. 2012). Importantly, data governance specifies security policies, standards, and obligations in an HIE. Therefore, it could be effective in countervailing security risks in data sharing. Nevertheless, little empirical evidence has shed light on how a hospital's data breach risks change after joining an HIE.

To address this gap in research, we propose the main research question for this study: *Does joining a Health Information Exchange affect a hospital's overall data breach risks?* To investigate the question, we first set up an analytical model to examine how the equilibrium of a hospital's IT security investment and security breach risks shifts when the hospital joins an HIE. Guided by the results of the model, we conduct a series of empirical analyses by compiling a six-year (2010-2015) panel dataset that covers comprehensive characteristics of hospitals and healthcare markets. We treat the staggered adoption of HIEs by hospitals as a quasi-experiment and use difference-in-differences (DiD) to evaluate how joining an HIE affects individual hospitals' breach risk. To mitigate endogeneity concerns, we leverage different identification strategies such as matching and instrument variables. Furthermore, we perform several robustness checks such as using Bacon decomposition, incorporat-

²<https://www.healthcareitnews.com/news/addressing-security-challenges-presented-hies>

³<https://www.securitymetrics.com/blog/how-healthcare-remains-insecure-and-what-one-hie-decided-do-about-it>

ing state-year fixed effect, and leveraging alternative models. Our primary findings remain consistent.

Our paper's main findings are as follows: First, contrary to prevalent concerns over data security in HIEs, we find that joining an HIE reduces the probability of hospitals' experiencing a data breach. Furthermore, we examine the main mechanisms through which hospitals' data security performance improves. Our analysis shows that a hospital increases its IT security investment after joining an HIE. We also find that hospitals' IT security capability moderates the relation between joining an HIE and security breach risk. Furthermore, we find that external law governing HIEs enhances HIE's security impact. Additionally, hospitals are less likely to experience IT system breaches and hacking after joining an HIE. However, we observe no significant changes in the likelihood of physical breaches and internal breaches.

We contribute to the information systems (IS) literature in several ways. This study is the first to analyze how joining HIE affects hospitals' data breach risks. It complements prior studies on the impact of digital practices on data security performance at organization levels. Furthermore, we consider the intensified threat of interdependent risks inherent to IOS usage and discuss how HIE governance could defend against the risks. It contributes to a stream of literature analyzing security breaches' negative externalities and related countermeasures. Finally, we contribute to the literature on IOSs, and to more broadly relationships between IOS implementation and data security. This topic has become critical in recent decades, given escalated IOS-related security issues, such as supply chain attacks and third-party breaches.

The study also offers practical implications for hospitals, HIE administrators, and policymakers. In particular, evaluating the impact of HIE on the healthcare data security landscape helps us better weigh the cost and benefit of the initiatives. Our findings support the effectiveness of HIE governance in reducing hospitals' breach risks. Both policymakers and HIE administrators should weigh these unexpected positive effects when funding and promoting HIE initiatives. Furthermore, we provide several suggestions for improving HIE governance, such as enhancing participants' IT

security capability, enforcing external policies, or introducing monitoring programs. Besides, we suggest that HIE security frameworks and standards can institute policies about effectively protecting physical equipment and raising employees' security awareness. Finally, our findings can shed light on other sectors where exchanging business-related or operational data through IOS is prevalent. Specifically, these IOS governance mechanisms and practices can plausibly be applied to different industries to enhance information security resilience in data sharing networks.

2.2 Literature Review

2.2.1 Interdependent Risks

Interdependent risks pose substantial threats to the information security field. These type of risk suggests that several attacks can be propagated from one point to another through interconnected IT systems (Anderson and Moore 2006). For instance, malware and viruses can spread from a host to other vulnerable hosts in network systems. Similarly, software vulnerabilities can be exploited to harm a group of users (August et al. 2014). The distributed denial-of-service (DDoS) attack takes advantage of interdependent network systems by leveraging a collection of compromised devices from different areas to build botnets (Hui et al. 2017). Realized interdependent information security attacks, such as supply chain attacks, can cause severe consequences. In 2020, the products of SolarWind, a software company, added malicious code, which makes its clients, including Fortune 500 companies and US government agencies, vulnerable to hackers (Iyengar 2020). Furthermore, it is extremely challenging to defend against this type of attack without collaborative efforts from different parties (Geng and Whinston 2000).

To investigate interdependent information security risks, this stream of literature commonly uses theoretical models to examine users' incentives in investing in cybersecurity in interconnected systems. Related studies argue that security risks are magnified in interdependent IT systems due to a lack of protection on users (Anderson and Moore 2006, Andrews et al. 2014, Kunreuther and Heal 2003). Specifically,

users may engage in opportunistic behaviors when risks are shared, especially when they are not concerned with other users' losses in breach incidents (Varian 2006). Limited resources and capability in cybersecurity further weaken users' incentives to ramp up their security protection (Fang et al. 2014, Lee et al. 2016). However, there is a lack of empirical evidence that examines users' incentives and incorporates contextual factors such as organizational and institutional characteristics, which hinders understanding how theories enlighten real-world practices.

We add to the stream of literature by connecting protection incentive models and empirical evidence in the setting of inter-organizational systems (IOS). First, we construct a stylized model where hospitals decide levels of IT security protection. Leading by results obtained from the analytical model, we compile an innovative dataset and conduct empirical analyses. Health Information Exchange is a typical IOS that enables data sharing among hospitals. Therefore, it's an appropriate context to examine interdependent risks.

2.2.2 Inter-organizational Systems and Governance

Inter-organizational systems (IOS) enable efficient data exchange across organizational boundaries (Bakos 1991), reducing communication frictions and lowering transaction costs (Malone 1987, Wang and Seidmann 1995). Unlike most information systems operating within a single organization, IOSs integrate IT systems from multiple unaffiliated organizations with varying objectives and processes. Hence, their implementation and collaborative usage may experience substantial challenges that hinder beneficial outcomes (Hamre and Monteiro 2013). One way to overcome these challenges is to institute IOS governance, a controlled structure that can facilitate agreements and realizations of IOS's value (Grover and Kohli 2012).

The literature categorizes IOS governance into different groups, such as contractual governance and relationship governance (Chatterjee and T.Ravichandran 2013, Fischer et al. 2012, Poppo and Zenger 2002). These governance mechanisms can increase IOS effectiveness, which is partially accomplished by specifying obligations

and establishing norms of cooperation (Larson 1992, Poppo and Zenger 2002). Additionally, IOS governance determines technical standards across organizations and information systems to ensure interoperability and efficient electronic data sharing (Gasparas and Monteiro 2009). Focusing on the same context as ours, Adjerid et al. (2018) find that IOS governance in HIE setting can effectively reduce Medicare spending in healthcare markets by enabling efficient transfer of health data across different healthcare providers. which reduce participants' opportunistic behaviors in transactions

Prior studies usually examine IOS governance in enhancing mutual benefits in IOS. However, the role of IOS governance in influencing security risks is seldom discussed. In other words, whether or not IOS governance can induce adequate protections in IOS participants is an unaddressed question. This question is crucial when information security risks are perceived as significant risks in IOS. Our study tries to answer the question by looking into HIE in the US healthcare sector where health data is stringently regulated and by examining the antecedent role of joining HIE on hospitals' realized data security risks.

2.2.3 Organizational IT Practices and Information Security

The information systems (IS) literature extensively investigates organizational security postures from the perspectives of primary security protection practices (Straub and Nance 1990) and security compromise paths (Ransbotham and Mitra 2009). Our study is close to the studies which examine how specific IT practices affect organizational data security risk (Kim and Kwon 2019, Kwon and Johnson 2014, Miller and Tucker 2011).

In the healthcare sector where data is of high risk, it is especially critical to examine the impact of new IT practices on hospitals' breach risks. Kim and Kwon (Kim and Kwon 2019) found that the adoption of Electronic Health Record increases hospitals' accident risks because of the digital disruptions in operations and workflows. Similarly, hospitals that pursue digitization required by meaningful-use attestation

may observe a short-term increase in data breach risks (Kwon and Johnson 2018). Furthermore, using IT security applications may not help reduce data security risks since the effectiveness of the protection practices is contingent on data management policies (Miller and Tucker 2011). As one of the most important healthcare digitization initiatives, HIE has tremendous implications for the healthcare service. However, how adopting or joining HIE as a type of IOS, affect a hospital’s data breach risks has never been formally and empirically tested in the literature.

Although a few studies empirically examine the impact of IOS on organizational cybersecurity, their findings are contradictory. Tanriverdi et al. (2019) use evidence from public firms’ to show that establishing external IT interlinkages with other firms weaken its security performance due to its increased structural complexity. On the contrary, Baskerville et al. (2018) leverage data on French firm and show that a firm with a higher level of external IT system integration use more cybersecurity countermeasures. They use vulnerability point theory to explain that external IT system integration exposes more controllable vulnerabilities, thereby inducing a greater IT security investment. Our study strives to gain a further understanding of the question. Specifically, we infer mechanisms by investigating different types of contingencies and security outcomes.

2.3 HIEs and Data Security

An HIE system or network is an electronic network that facilitates electronic health information sharing between healthcare providers. Most HIEs are administered by third-party technology service organizations such as regional health information organizations (RHIOs).⁴ As a typical inter-organizational system, an HIE relies on the combination of technologies and a trusting community. To theorize the impact of joining in an HIE hospitals’ breach risks, we discuss the information security implications of an HIE from both risks and governance perspectives.

⁴HIEs can be categorized based on different dimensions. For example, according to the HIE convener, HIE can be categorized as three main types of HIEs: community HIE, enterprise HIE, and (EHR) vendors HIE (Everson 2017; Vest et al. 2013). Our study does not focus on different types of HIEs.

2.3.1 Data Breach Risks in Joining an HIE

The public has expressed concern regarding HIEs' ability to handle their health data securely. These concerns are likely borne out of several factors related to the increased breach risks in hospitals after they join an HIE. First, joining an HIE increases the volume of data present in hospitals, making hospitals attractive targets for attackers. When hospitals need information about patients, they can retrieve and store other hospitals' data from the HIE network; and make their own data accessible to other members of the same HIE network. As a result, data from disparate departments or labs across many health organizations are digitalized and transferred to a hospital's IT systems in aggregate. The payoffs of infiltrating and getting illegal access to the data increase since these operations increase the amount of accessible healthcare data in a hospital. Therefore, malicious attackers are more likely to target the hospital.

Second, changing IT applications and increased data access can increase hospitals' risk. To enable data sharing through an HIE, a hospital needs to update or even change its main health IT systems (Feldman et al. 2014), some of which may bring in security flaws that render internal IT systems more vulnerable. This is especially salient given that a hospital is limited in its ability to identify and remediate these digital threats. Furthermore, a hospital collects health data from different departments, which opens more data access points for potential unauthorized breaches without sufficient protection (Wang et al. 2015). Additionally, the digital transformation introduced by HIE may disrupt data processing routines and employees' workflows (Adler-Milstein et al. 2011), increasing the likelihood of data misuse (D'Arcy et al. 2020).

Third, if the HIE network link is vulnerable to illegal access and attack in transmission channels, other participants in the same HIE network may become sources of attacks. This link weakness may also increase attackers' capabilities because they can strategically exploit the weakest point to get illegal access to another system (Hui et al. 2012, Zhao et al. 2013). Although there is no detailed information on this type

of risk in terms of the attacking source and the indirect attack victims, we cannot exclude the possibility that some attackers may bypass detection or eliminate traces of their access. Therefore, we assume that these types of attacks are captured in hospitals' data breach outcomes.

2.3.2 HIE's Data Security Governance

Data security protection is a critical part of IOS governance in an HIE network. In 2008 and 2013, the Office of the National Coordinator for Health Information Technology (ONC) released documents on the HIE framework and emphasized security protection. In practice, HIE stakeholders decide on the governance framework during the planning phase and implement practices in the operational phase (Adjerid et al. 2018). We summarize these practices through the lens of network security.

HIE governance ensures a participating hospital's security protection by increasing their data security awareness and imposing accountability for security incidents. According to the HIPAA Privacy Rule, hospitals need to sign Participant Agreements (PAs) when joining an HIE. These agreements are concrete and enforceable to ensure that all necessary security and privacy requirements are met for each participant (HHS 2015). In particular, HIE participants need to comply with data usage policies to protect data privacy and integrity. For example, it is necessary to ask for patients' permission when sharing their data. Also, HIE governance promotes risk assessment which helps hospitals identify their risks (AHIMA/HIMSS 2011, McGowan et al. 2012, NIST 2010).

Furthermore, HIE governance holds participants accountable for their security breaches. In an IOS, interdependence across organizations may exaggerate the risks and severity of data securities incidents. This interdependence may also lower organizations' incentives in investing in security measures (Ogut et al. 2004). HIE governance can mitigate the issue by internalizing the costs of security breaches. Specifically, the assigned accountability of data misuse binds HIE participants in agreements. If a data breach occurs, the focal participant must notify other par-

ticipants and take proper measures to cure breach incidents. Otherwise, HIEs may terminate data sharing with uncooperative participants.⁵ Moreover, if a participant's security negligence is a massive breach, other participants may bring it to court, internalizing losses and deterring and reducing opportunistic behaviors.

Lastly, HIE governance standardizes technical specifications to ensure data access and transmission security. Providing a high level of verification and authentication between various entities during the data sharing process is critical (Snell 2015). Considering unauthorized access to the HIE portal may affect the whole HIE network; therefore, it is essential to implement stringent data access policies and technologies to prevent risks. In a further step, the technical infrastructure of data transmission enables HIE administrators to monitor data exchange activities via the system (NIST 2010). Hence, they can audit participants' historical data access records and identify abnormalities in the data sharing processes. Also, data transmissions in HIEs follow the privacy and security standards embedded in HIE functionalities. For instance, two widely used health data exchange standards, Direct and Fast Healthcare Interoperability Resources (FHIR), implement several protocols to secure data transmission.

2.4 Theoretical Framework

In this section, we develop a theoretical framework to determine mechanisms by which joining an HIE impacts a hospital's data breach risks. We assume that hospitals are rational agents when they decide the level of efforts in protecting data security. Based on the framework, we theoretically analyze the following questions:

1. *How does joining HIE affect hospitals' data breach risks?*
2. *How do hospital-level factors (i.e., the unit cost of protection) and HIE-level factors (i.e., the effectiveness of HIE governance) affect the changes in data breach risks?*

⁵See examples in public HIE agreements: <https://mehi.masstech.org/sites/mehi/files/documents/MassHIway-Participation-Agreement.pdf>, <https://www.provshare.org/documents/HIE/PSJH-HIE-Participation-Agreement-47287635-v7.6.pdf>

To answer these questions, we consider two scenarios in the model: a baseline case in which two hospitals (Hospitals A and B) do not share data with each other, and another where the two hospitals exchange their data. For simplicity, we assume that the decision to exchange data is exogenous and the two hospitals are identical in terms of sizes, protection costs, and other characteristics. To protect their digital assets, the hospitals each make investments that raise the level of cybersecurity protection (C_i). This investment is an increasing function of the protection level (p_i). Specifically, it is given by

$$C_i = \frac{1}{2}cp_i^2 \quad i \in (A, B) \quad (1)$$

where c is the unit cost of protection that is assumed to be positive. As shown in Eq.1, C_i is a convex function of p_i , which is a common cost structure in security investment models (August et al. 2014, Lee et al. 2013). A hospital incurs costs during both security losses and protection investment, and the main objective is to minimize the total cost.

2.4.1 A Baseline Case

In the baseline case, the two hospitals do not share information. We posit that the probability of a breach I_{0i} for hospital i is given by

$$I_{0i} = B_0 - \beta p_{0i} \quad (2)$$

where B_0 refers to the level of threats in the absence of any security protection for either hospital. The amount of expected damage is a function of the breach probability and given by αI_{0i} where α refers to the damage (cost) that the hospital would suffer from a security breach. The organization's objective function is given by

$$\min_{p_{0i}} R_{0i} = \alpha I_{0i} + C_i = \alpha (B_0 - \beta p_{0i}) + \frac{1}{2}cp_{0i}^2. \quad (3)$$

It chooses the level of protection (p_i) that minimizes the total cost R_{0i} . Solving the first-order condition $\frac{\partial R_{0i}}{\partial p_{0i}} = 0$ gives

$$p_{0i}^* = \frac{\alpha\beta}{c} \quad (4)$$

Also, the second-order $\frac{\partial^2 R_{0i}}{\partial^2 p_{0i}} > 0$. The breach probability in the baseline case is:

$$I_{0i}^* = B_0 - \frac{\alpha\beta^2}{c} \quad (5)$$

2.4.2 A Case with Information Exchange

Next, we examine the case in which the two hospitals agree to exchange their information via an HIE. Our model focuses on the two hospitals' security investment choices given the exchange decision and the resulting security risks.

In this scenario, we argue that the probability of an intrusion into one hospital depends on not only the amount of data it possesses and the level of its security protection ($p_{1i}, i \in (A, B)$) but also the level of security of its counterpart, which is a typical example of "interdependent security" (Kunreuther and Heal 2003). This is because by exchanging the information, the hospital bears a risk of breaches of its digital assets that might take place at either its own system or the other system. Specifically, in the two-hospital network, an infiltrator that breach the system of hospital A may attempt to gain access to data from hospital B via the data exchange channel between A and B. This type of risk is common in the network setting (Acemoglu et al. 2016, Lee et al. 2016). Importantly, we consider the effectiveness of HIE governance (γ) as a way to enhance hospitals' protection and lower the indirect risk.

Taking all these attack possibilities into account, we characterize the probability of intrusion for hospitals A and B in the presence of information exchange as follows:

$$I_{1i} = B_1 - (\beta p_{1i} + \gamma p_{1i} p_{1j}) \quad (i, j \in \{A, B\}) \quad (6)$$

As in the Eq.2, B_1 refers to the level of threats in the absence of any security protection.

Assumption 1. $B_1 > B_0$

We introduce *Assumption 1* because each of the two hospitals' data volume and data access increase after they exchange and store data from both, as discussed in Section 2.3.1 According to Rational Choice Theory, attackers are rational in deciding to commit crimes by calculating the benefits and costs of intrusion (Becker 1968). Given other things being equal, they are more likely to attack organizations with more digital assets (Wang et al. 2015). In our context, the theory suggests the amount of patient data that a hospital owns or has access should be positively associated with breach risks.⁶

The second term in Eq.6, βp_{1i} , represents prevention of direct attacks against hospital A or B. The third term, $\gamma p_{1i} p_{1j}$, indicates prevention of an indirect attack to the system of A through B or vice versa. In a scenario wherein hospital B fails to deter attacks due to insufficient protection (low p_{1B}), hospital A can still prevent an indirect attack through B by raising its protection level (high p_{1A}).

The hospitals choose a positive level of protection in equilibrium. As in the baseline case, the organization determines the protection level (p_{1i}) that minimizes the sum of the expected damage (αp_{1i}) and the protection cost (C_i).

$$\min_{p_{1i}} R_{1i} = \alpha I_{1i} + C_i = \alpha(B_1 - \beta p_{1i} - \gamma p_{1i} p_{1j}) + \frac{1}{2} c p_{1i}^2 \quad (7)$$

Solving the first-order conditions results in a Nash equilibrium of the two organizations' security protection level, we obtain ⁷

$$p_{1i}^* = \frac{\alpha\beta}{c - \alpha\gamma} \quad (8)$$

The breach probability in this case can be written as

$$I_{1i}^* = B_1 - \frac{\alpha\beta^2 c}{(c - \alpha\gamma)^2} \quad (9)$$

⁶Our empirical results in Table 4 support the argument by showing the statistically significant positive association between internal health system size and data breach risks.

⁷. p_{1i}^* is positive by Assumption 2. $c - \alpha\gamma > 0$

2.4.3 Comparison of the Two Cases

In this section, we compare the two cases above (the absence and presence of information exchange) to derive security implications from establishing the exchange. To answer the two main questions mentioned above, we first examine changes in the optimal security level that the two hospitals would choose in equilibrium depending on the two cases. We find that,

Lemma 1. After establishing information exchange, both hospitals increase the level of security protection, as given by $p_{1i}^ > p_{0j}^*$.*

Compared to Eq.4 (i.e., $p_{0i}^* = \frac{\alpha\beta}{c}$) and Eq.8 (i.e., $p_{1i}^* = \frac{\alpha\beta}{c-\alpha\gamma}$), we can see that the hospital increases its security protection investment. We also find

$$\frac{\partial p_1(*)}{\partial \gamma} = \frac{\alpha^2\beta}{(c-\alpha\gamma)^2} \quad (10)$$

In other words, the more effective HIE governance (γ) is in improving protection against indirect attack, the higher the level of protection the hospital is incentivized to pursue. Next, we explore *how joining an HIE affect the data breach risks* by comparing the predicted probability of intrusions (I_{0i}^* and I_{1i}^*) and we obtain. We find the change is

$$I_{1i}^* - I_{0i}^* = B_1 - \frac{\alpha\beta^2c}{(c-\alpha r)^2} - B_0 + \frac{\alpha\beta^2}{c}$$

Lemma 2. After establishing information exchange between the two hospitals, the probability of data breaches decreases ($I_{1i}^ < I_{0i}^*$) if and only if the effectiveness of governance (γ) is sufficiently high (i.e., $\gamma > \frac{(c)(1-\frac{\beta\sqrt{\alpha H}}{H})}{\alpha}$), where $H = \alpha\beta^2 + (B_1 - B_0)c$.*

According to our derived results, the hospital's data breach risks decrease if HIE governance is effective (high γ). There are two channels through which the effect is realized. First, HIE governance directly reduces the indirect attack (via HIE) given the same protection levels. Second, it incentivizes a hospital to increase its security protection level, leading to a decrease in the direct attack risks.

Next, we explore the second question: *how do hospital-level factors (i.e., the unit cost of protection) and governance-level factors (i.e., the effectiveness of governance)*

affect the changes in data breach risks? Specifically, we examine how the focal hospital's unit cost of security protection (c) and the effectiveness of governance (γ) affect the changes in the probability of data breach risks ($I_{1i}^* - I_{0i}^*$). Based on previous results, we derive the following Lemmas:

Lemma 3. If breach risks decrease after exchanging information ($I_{1i} - I_{0i} < 0$),

(a) the magnitude of the decrease is negatively associated with the hospital's security protection cost (c) (i.e., $\frac{\partial |I_{1i}^ - I_{0i}^*|}{\partial c} < 0$).*

(b) the magnitude of the decrease is positively associated with the effectiveness of HIE governance (γ) (i.e., $\frac{\partial |I_{1i}^ - I_{0i}^*|}{\partial \gamma} > 0$).*

Lemma 4. If breach risks increase after exchanging information ($I_{1i} - I_{0i} > 0$),

(a) the magnitude of the increase is positively associated with the hospital's security protection cost (c) (i.e., $\frac{\partial |I_{1i}^ - I_{0i}^*|}{\partial c} > 0$).*

(b) the magnitude of the increase is negatively associated with the effectiveness of HIE governance (γ) (i.e., $\frac{\partial |I_{1i}^ - I_{0i}^*|}{\partial \gamma} < 0$).*

First, we consider the case when a hospital's data breach risks decrease. Specifically, the extent to which joining an HIE reduces data breach risks is contingent on two key variables: the unit cost of protection (c) and the effectiveness of HIE governance (γ). According to *Lemma 3a*, if a hospital has a lower unit cost of data protection, the benefit of decreasing the losses of data breaches outweighs the data protection expenditure. Hence, the hospital has an incentive to allocate more resources in data protection, leading to a larger magnitude decrease in breach risks. Furthermore, *Lemma 3b* reveals the importance of effectively lowering inter-dependent risks. Specifically, the decrease in individual hospitals' breach risks is more substantial when the link protection is more effective. Effective governance could not only reduce the indirect risks, but also internalize the losses of data breaches in IOS systems like HIE. Therefore, the focal hospital is more likely to increase data protection spending considerably to improve its security at a larger magnitude.

Furthermore, we consider the case that joining HIE may increase a hospital's data breach risks. The magnitude of the heightened risks would increase if security

protection cost is higher (*Lemma 4a*), or it would decrease if the governance is more effective (*Lemma 4b*). We paraphrase all *Lemmas* and summarize them in Table 2.1.

Table 2.1. A Summary of Lemmas

Number	Lemma
1	After joining HIE, a hospital increases IT security investment.
2	Joining HIE may or may not increase data breach risks.
3a	If joining HIE lowers data breach risks, the impact would be reduced on hospitals with a higher unit cost of protection.
3b	If joining HIE lowers data breach risks, the impact would be enhanced when the effectiveness of IOS governance increases.
4a	If joining HIE increases data breach risks, the impact would be enhanced on a hospital with a higher unit cost of protection.
4b	If joining HIE increases data breach risks, the impact would be reduced when the effectiveness of IOS governance increases.

2.5 Data Description

To empirically analyze the main research questions, we construct a six-year (2010-2015) panel dataset of more than 3,000 hospitals in the United States. We choose 2010 as the starting year for two primary reasons. First, as part of the American Recovery and Reinvestment Act of 2009, several health data breach notification rules were introduced, including the Federal Trade Commission (FTC) Health Breach Notification Rule ⁸ and the Department of Health and Human Services (HHS) Breach Notification for Unsecured Protected Health Information.⁹ Second, the earliest reported date of breach incidents in the official HHS breach portal is October 2009.¹⁰

⁸16 C.F.R. § 318.

⁹45 C.F.R. § 160.164.

¹⁰https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=462449A03A8E32E25A201EFE68974C80

These facts ensure that data after 2010 capture a complete snapshot of hospitals' breach incidents.

We collect data from multiple sources, including (1) security breaches from the Privacy Rights Clearinghouse and The U.S. Department of Health and Human Services (HHS) breach portal; (2) hospitals' characteristics and IT practices from the HIMSS Analytics data; (3) Meaningful use attestation status from CMS website;¹¹ and (4) health referral region characteristics from Dartmouth Health Atlas (DHA) and U.S. Bureau of Labor Statistics. We report the main variables' summary statistics in Table 4.1 and their correlation matrix in Table A.1 (Chapter 4).

2.5.1 Outcome and Treatment Variables

The main outcome variable in our study is the occurrence of data breach incidents. We collect hospitals' security breach incidents from two sources, including the Privacy Rights Clearing House and the U.S. Department of Health and Human Services (HHS), which have been commonly used in previous research (Kwon and Johnson 2014, 2018, Angst et al. 2017). The dataset provides detailed information on each incident, such as breached hospital names, breach dates, breach types, and the number of affected records. After merging the hospital and breach incident data, we can identify each breached hospital. The mean value of DataBreach is 0.04 in our sample, which suggests that 4% of observations in our sample experienced at least one data breach between 2010 and 2015.

The treatment variable is HIE status, i.e., whether or not a hospital joins in HIE. We collect data on hospitals' HIE statuses from the HIMSS Analytics database which has been widely used in healthcare IT studies (Angst et al. 2017, Kwon and Johnson 2014, Miller and Tucker 2009). The dataset features a binary indicator for whether hospitals join HIEs.¹² Figure 2.1 presents the map of HIE state-level participation

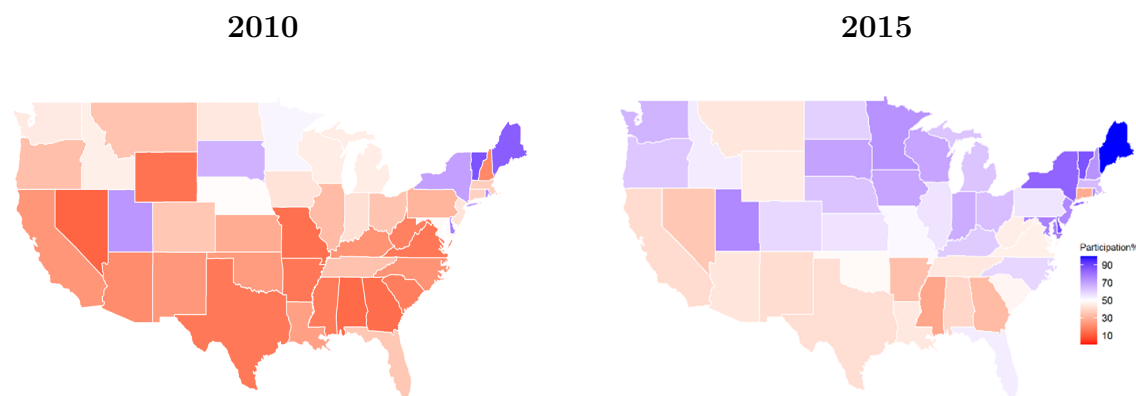


Figure 2.1. HIE Participation Rates

rates in 2010 and 2015. The changes in the HIE statuses of hospitals comprise the main variations in our analyses.

2.5.2 Control Variables

We first collect data on hospital-level characteristics that are likely to affect hospitals' data breach risks. First, we consider hospitals' basic information, including the number of beds in a hospital's health system (measures of the size of digital assets) and the operating expense (measures of financial performance). We also consider hospitals' IT characteristics, including the number of operational IT applications, as measures of IT capability. This is because IT complexity or capability is plausibly associated with data security risks. Similar to previous studies (Miller and Tucker 2011; Burke and Menachemi 2004), we categorize health IT applications into different types

¹¹Centers for Medicare & Medicaid Services: <https://www.cms.gov/>.

¹²We exclude hospitals which do not meet two criteria: 1. have observations for the six-year period 2010-2015 in HIMSS data, 2. have at least three-year consecutive HIE status. In addition, HIE information is missing in 2011 from HIMSS data. However, using data from 2010 and 2012, we make some reasonable assumptions about HIE membership in 2011. If a hospital was part of an HIE in 2010 and 2012, we assume it was part of an HIE in 2011. Similarly, if a hospital was not part of HIE in 2010 and 2012, we assume it was not part of an HIE in 2011. If a hospital's HIE participation statuses in 2010 and 2012 are different or missing, we remove its 2011 data from our analysis.

based on their functionalities – clinical applications, administrative applications, and strategic applications and incorporate them in our analyses. During the sample period, the Centers for Medicare and Medicaid Services (CMS) introduced meaningful-use (MU) attestation to facilitate EHR assimilation into clinical workflows (Kwon and Johnson 2018). The attestation requires healthcare providers to establish systematic procedures to improve service quality and security posture (Kwon and Johnson 2018). Therefore, hospitals with incentives to reach the MU standard are likely to join an HIE and take measures to improve data protection. To eliminate the confounding effect of MU attestation, we incorporate MU status as a control variable in our model.

HIE participation also depends on regional characteristics, including competition, healthcare complexity, and economic conditions. First, hospitals in more competitive markets are more sensitive to potential gains from owning patients’ data. As a result, they are less likely to join an HIE (Adler-Milstein and Jha 2014). Similarly, competition also influences hospitals’ investment strategy, which includes information security investment (Gaynor et al. 2012). Second, economic conditions may also affect hospitals’ digitization decisions. Some regional shocks, such as policy interventions or economic recessions, could influence the establishment of HIE and hospitals’ strategies at the same time. To capture those effects, we consider related characteristics at the Hospital Referral Region (HRR) level as the regional healthcare market (Adjerid et al. 2018). We also use an HRR-level Herfindahl-Hirschman Index (HHI) to proxy competition. Following previous practices (Gaynor et al. 2012), we obtain HRR data from the Dartmouth Health Atlas (DHA) and identify 306 HRRs across the United States. Then, we use the number of hospital beds as a proxy of hospitals’ size and calculate its proportion of the total size in the HRR as its market share, and HHI is the sum of squared of market shares for all hospitals in the same region. We also capture healthcare complexity by using HRR Case Mix Index.¹³

Furthermore, we incorporate HRR-level income, population, and unemployment. The data are from multiple sources, including The U.S. Department of Housing and Urban Development (HUD) and the Census Bureau. Next, we follow practices in

¹³The dataset is from Dartmouth Health Atlas.

Table 2.2. Summary Statistics

Variable	Description (hospital i , hospital referral region h , state s at year t)	Mean	SD	Sources
Outcome Variables				
Data Breach _{it}	Binary indicator for whether a hospital i experiences data breaches at year t	0.04	0.21	Privacy Rights Clearinghouse, HHS breach portal
Treatment Variable				
Join HIE _{it}	Binary indicator for whether a hospital i joins an HIE at year t	0.41	0.49	HIMSS
Other Variables				
Size _{it}	Log of the number of beds in a health system size	6.77	2.12	HIMSS
Operation Expense _{it}	Log of the total amount of operational expenses	18.01	1.39	HIMSS
IT Apps _{it}	Log of the total number of live apps	4.09	0.40	HIMSS
Admin Apps _{it}	The total number of live administrative apps	19.91	4.81	HIMSS
Strategy Apps _{it}	The total number of live strategy apps	10.97	4.20	HIMSS
Clinic Apps _{it}	The total number of live clinic apps	22.21	8.85	HIMSS
MU1 _{it}	Binary indicator for whether a hospital achieved Meaningful Use stage 1	0.31	0.46	CMS
IS Plan _{it}	Binary indicator for whether a hospital has information system strategic plans	0.71	0.45	HIMSS
MSA _i	Binary indicator for whether a hospital is in a metropolitan area	0.69	0.46	HIMSS
Academic _i	Binary indicator for whether a hospital is academic	0.05	0.21	HIMSS
ForProfit _i	Binary indicator for whether a hospital is for-profit	0.19	0.39	HIMSS
HHI _{ht}	The competition index (HRR)	7.22	0.76	Dartmouth Health Atlas
CMI _{ht}	The case mix index (HRR)	1.48	0.14	Dartmouth Health Atlas
Income _{ht}	Log of Per capita income (HRR)	10.62	0.25	HUD, Census Bureau
Population _{ht}	Log of the population (HRR)	11.94	1.88	HUD, Census Bureau
Unemployment _{ht}	Unemployment rate (HRR)	2.09	0.31	HUD, Census Bureau

previous studies to measure HRR-level variables (Adjerid et al. 2018; Fu et al. 2013). Specifically, we use two crosswalk files provided by DHA and HUD to map zip-code, county, and HRR, then calculate a weighted average for each variable.

2.6 Empirical Specifications

2.6.1 Difference in Differences

Our main objective is to estimate how joining an HIE affects the likelihood that hospitals experience data breaches. The key variable of interest is whether a hospital participates in an HIE during a given time period. In our context, hospitals' staggered HIE adoptions provide a quasi-experiment setting and enable us to evaluate the effect with a difference-in-differences (DiD) approach. We estimate linear probability models (LPM) with two-way fixed effects for two primary reasons. First, using LPM enables us to avoid the incidental parameters problem, which causes inconsistency in a non-linear model with fixed effects (Miller and Tucker 2009). Second, the results are generally consistent with estimates in non-linear models and are more interpretable (Angrist and Pischke 2008). The specification of the baseline model is as follows:

$$DataBreach_{it} = f(JoinHIE_{it}, X_{it}, \gamma_i, \mu_t, \epsilon_{it})$$

In the specification, the outcome variable $DataBreach_{it}$ indicates whether a hospital i experiences at least one security breach in year t . Our primary variable of interest is $JoinHIE_{it}$, which captures whether a hospital i is a member of an HIE in year t . Furthermore, we incorporate a vector of time-varying characteristics of hospitals X_{it} . Besides, γ_i and μ_t are hospital and year fixed effects. Hospital fixed effects allow us to control for time-invariant heterogeneity across different hospitals. Year-fixed effects capture time trends. Lastly, ϵ_{it} represents independently and identically distributed errors. We report robust standard errors clustered at the hospital

level. Since clustering can be viewed as an experimental design issue (Abadie et al. 2017), it is reasonable to cluster at the unit where the treatment was assigned.¹⁴

2.6.2 Matching Strategies

In our context, because hospitals can choose whether or not to join HIE, self-selection is a concern. In other words, some hospital-level confounding factors may affect the decision to join HIE and data breach risks. For instance, hospitals’ governance structures can affect digitization decisions, confounding HIE’s impact on data breach risks. To further alleviate endogeneity concerns, we use matching strategies that are commonly implemented in empirical studies on hospitals (Ayer et al. 2019, Kwon and Johnson 2018, Sun et al. 2020). Matching is useful in the health context where significant disparities exist among U.S. hospitals in terms of financial performance and digital capabilities. Effective matching can construct a sample with a “better balance between the treated and control groups” (Iacus et al. 2012). In our case, the assignment of the treatment (i.e., Joining HIE) should resemble a randomized experiment after effective matching.

First, we use Propensity Score Matching (PSM). This approach leverages observable covariates to identify a non-treated unit (i.e., Not in HIEs) that would have been most likely to have been treated (i.e., Joining HIEs). These covariates include hospitals’ institutional characteristics, IT practices, and market competition indicators. We use the pre-treated mean of those covariates to estimate hospitals’ propensity score of joining HIEs. We also incorporate variables that do not frequently change over time, including MSA_i (if a hospital is in a metropolitan statistical area), $Academic_i$ (if a hospital is focused more on academic research and teaching), $ForProfit_i$ (if a hospital is a for-profit), since they are essential factors in hospitals’ health IT strategies (Angst et al. 2017).

Next, we keep observations that are matched based on propensity scores. We perform the probit regression and K-nearest-neighbor matching (K=3) with a caliper

¹⁴We also use standard errors clustered at the state level and the hospital referral regional level. Similarly, the results are statistically significant at the 5 % level or 10% level.

Table 2.3. Propensity Scores Matching – Descriptive Analyses

Variable	Before Matching				After Matching			
	Treated	Control	Bias%	p-value	Treated	Control	Bias%	p-value
Health System Size	6.75	6.86	-4.90	0.27	6.72	6.67	2.40	0.61
Operation Expense	18.13	17.70	32.90	0.00	18.10	18.12	-1.60	0.75
IT Apps	4.12	4.00	42.30	0.00	4.11	4.12	-0.60	0.85
IT Security Apps	3.81	3.93	-8.10	0.06	3.85	3.84	1.30	0.80
Admin Apps	20.01	19.04	27.80	0.00	19.95	19.94	0.20	0.98
Strategy Apps	11.22	9.82	40.70	0.00	11.05	11.04	0.30	0.95
Clinic Apps	22.78	19.74	39.0	0.00	22.62	22.91	-3.8	0.41
MU1	0.29	0.29	0.60	0.89	0.30	0.31	-5.6	0.25
IS plan	0.73	0.70	15.8	0.00	0.73	0.71	4.5	0.37
MSA	0.72	0.64	17.90	0.00	0.71	0.68	7.9	0.11
Academic	0.05	0.02	16.1	0.00	0.04	0.05	-2.4	0.11
For profit	0.14	0.34	-48.3	0.00	0.15	0.13	4.0	0.34
Competition	7.20	7.24	-5.3	0.23	7.22	7.19	3.4	0.51

size of 0.01 and present descriptive analyses of covariates in Table 2.3. Before matching, there are substantial differences between the treated group and the control group. Hospitals in HIEs are more likely to be not-for-profit, academic, in metropolitan areas, and have a higher level of digitalization. The outcomes are consistent with the literature on HIE participation (Adler-Milstein and Jha 2014, Adler-Milstein et al. 2011). After matching, the difference between the treated and control groups is insignificant across all covariates, suggesting that our matching strategies generate a balanced sample in which hospitals in the treated group and the control group share similar characteristics. Therefore, our estimation is less likely to be biased after using the matched sample.

2.7 Analyses

To investigate the mechanisms driving the effect of joining an HIE on hospitals' data security, we empirically test the Lemmas from our analytical model in Table 2.1.

2.7.1 IT Security Investment

As per *Lemma 1*, hospitals tend to increase IT security investment after joining HIEs. Consistent with studies on IT security in organizations (Angst et al. 2017, Kwon and Johnson 2014) we use the number of adopted IT security applications as proxies for IT security investments. In the HIMSS database, we capture various IT security applications, including encryption, firewall, single sign-on, spam/spyware filter, fingerprint scanning, and ten other IT applications.¹⁵

We first use OLS to estimate the impact of joining HIE on the number of adopted IT security applications. Since the number of adopted IT security applications is a count variable, we also use a Poisson quasi-maximum likelihood estimator (PQML), which is commonly used in previous studies (Dobkin et al. 2018, Greenwood and Wattal 2017). The estimator has several benefits. First, it allows for the creation of robust standard errors. Second, it does not require that the dependent variable's distribution must be Poisson or negative binomial. To refine the analysis, we use a matched sample in the estimation. The results in Table 2.4 present that the coefficient of $JoinHIE_{it}$ is significantly positive, suggesting that a hospital adopts more IT security technologies after joining an HIE, thus supporting *Lemma 1*. However, increasing IT security investment does not necessarily lead to better security performance. As our theoretical framework suggests, security threats increase after a hospital joins HIE. Even though a hospital adopts more security applications, the increased protection may not offset the heightened threats. Therefore, it is critical to empirically test how joining an HIE affects data breach risks.

¹⁵These IT security apps cannot represent a hospital's total IT security investment including employee's security awareness training, security maintenance. Therefore, the results need to be interpreted with cautions.

Table 2.4. The Impact of Joining HIE on Hospital's IT Security Investment

	(1)	(2)
DV: No. Adopted IT Security Apps	OLS	PQML
Join HIE	0.386*** (0.059)	0.046*** (0.012)
Constant	2.152 (5.767)	
R-squared/Log likelihood	0.788	-10323.695
Observations	8504	8504
No. Hospitals	1637	1637
Hospital & Year FE	YES	YES
Control Variable	YES	YES

Notes: All estimations use cluster-adjusted robust standard errors (clustered at the hospital level).

We use a matched sample in these analyses. *** $p < 0.001$, ** $p < 0.01$, * $p < 0.05$, + $p < 0.1$

2.7.2 Data Breach Outcomes

Lemma 2 in our theoretical framework suggests that joining an HIE may or may not increase data breach risks, depending on the effectiveness of HIE governance. We present the main results of our empirical analysis in Table 2.5. The results report a significant negative association between HIE participation and data breach occurrences. In Column (1), we use the full sample without control variables and find a hospital's data breach probability decreases by 1.9 percentage points after joining an HIE. Column (2) shows that the results of a model with all control variables are similar to those in Column (1). Next, we use the matched sample to estimate the main effect with Difference in Differences and report results in Columns (3), (4), and (5).

After using PSM ($K = 3$), the R-squared increases in the matched sample results, showing the model fitness improves. Column (3) shows that the coefficient of JoinHIEs is -0.017 , suggesting that the data breach likelihood decreases by 1.7 percentage points if a hospital joins an HIE. Considering that the mean value of the data breach indicator in our sample is 0.04, the magnitude of reduction is around 43% ($0.017/0.04 = 0.425$). In case the results are sensitive to different matchings, we use another matching with $K = 5$ and obtain a new sample. Results in Columns (4) are similar to the previous analyses.

In a further step, we use Coarsened Exact Matching (CEM) as an alternative matching strategy. CEM helps mitigate issues caused by human choices in PSM, since it does not require data generation process assumption (Iacus et al. 2012, King and Nielsen 2019). Hence, we use CEM to yield a new matched sample. Specifically, we first manually specify two bins for binary variables (e.g., academic, for-profit, MSA) and five bins for other variables (e.g., health system size, operation expense). Next, we use the CEM matched sample to estimate the main effect and report results in Column (5). We also incorporate CEM weights in estimations and present results in Column (6).¹⁶ All findings suggest that the likelihood of a hospital’s data breach decreases after it joins an HIE, showing the robustness of the results in different matched samples. While our theoretical model predicts either an increase or decrease in security breaches risks due to the presence of countervailing forces, we empirically observe the governance effect dominates such that the breach risks decrease when a hospital joins an HIE.

2.7.3 IT Security Capability

If the unit cost of protection is high, a hospital is less likely to improve data security after joining an HIE (*Lemma 3a* in the theoretical framework). If that is the case, we should observe that the unit cost of protection negatively moderates the impact of joining an HIE on a hospital’s data breach risks.

¹⁶We thank a reviewer for suggesting the analysis.

Table 2.5. The Impact of Joining HIE on Hospital's Data Breaches

DV: Data Breach	(1)	(2)	(3)	(4)	(5)	(6)
	Bivariate	Control Variables	PSM K =3	PSM K = 5	CEM	CEM Weights
Join HIE	-0.018** (0.006)	-0.018** (0.007)	-0.017* (0.007)	-0.017* (0.007)	-0.019* (0.009)	-0.023* (0.010)
Health System Size		0.025*** (0.004)	0.028*** (0.005)	0.027*** (0.004)	0.021*** (0.006)	0.022*** (0.006)
Operation Expense		-0.008 (0.009)	-0.006 (0.010)	-0.013 (0.010)	-0.003 (0.015)	0.018 (0.018)
IT apps		-0.097*** (0.023)	-0.078* (0.034)	-0.090** (0.031)	-0.055+ (0.033)	-0.064 (0.045)
Admin Apps		0.004*** (0.001)	0.004** (0.001)	0.005*** (0.001)	0.005** (0.002)	0.007*** (0.002)
Strategy Apps		0.002+ (0.001)	0.000 (0.001)	0.000 (0.001)	-0.000 (0.002)	-0.004 (0.003)
Clinic Apps		0.001 (0.001)	0.001 (0.001)	0.001 (0.001)	0.000 (0.001)	0.001 (0.001)
MU1		0.004 (0.004)	0.012* (0.006)	0.012* (0.005)	-0.002 (0.006)	-0.005 (0.007)
IS Plan		-0.018* (0.008)	-0.035*** (0.011)	-0.040*** (0.010)	-0.013 (0.012)	-0.008 (0.013)
HHI		-0.029 (0.023)	-0.041 (0.025)	-0.052* (0.023)	-0.064 (0.046)	-0.197* (0.089)
CMI		-0.066+ (0.034)	-0.119** (0.042)	-0.109** (0.038)	-0.069 (0.051)	-0.096 (0.058)
Income		-0.034 (0.035)	0.006 (0.045)	-0.004 (0.042)	-0.059 (0.047)	-0.070 (0.051)
Population		-0.000 (0.021)	-0.011 (0.019)	-0.000 (0.019)	-0.043 (0.032)	-0.030 (0.038)
Unemployment		-0.030 (0.021)	0.018 (0.027)	0.018 (0.025)	0.027 (0.031)	0.018 (0.046)
R-squared	0.244	0.249	0.287	0.286	0.266	0.270
Observations	19897	18159	9387	10301	5924	5924
No. Hospitals	3344	3215	1644	1805	1034	1034
Hospital & Year FE	YES	YES	YES	YES	YES	YES

Notes: All estimations use cluster-adjusted robust standard errors (clustered at the hospital level).

*** p<0.001, ** p<0.01, * p<0.05, +p<0.1

We use hospitals' IT security capability as a proxy for the unit cost of protection. According to absorptive capacity theory, an organization's prior experience and related knowledge contribute to new practices' performance (Roberts et al. 2012, Bharadwaj 2000, Cohen and Levinthal 1990). In particular, when hospitals experience increased threats and new compliance requirements (i.e., joining HIE in our context), the *prior investment in IT security* can affect the data protection costs for several reasons.

First, previous IT security investment provides employees with opportunities to increase data security awareness. Hence, employees may find it easier to adjust to and comply with the additional regulations that HIE governance introduces. Second, prior investment in IT security allows hospitals to develop protection procedures that enable administrators to adjust deployment and cope with influxes of data in a less costly manner after joining an HIE. Third, prior IT security investment enables organizations to leverage new IT security applications more efficiently. However, if hospitals are inexperienced in IT security management, they may implement new IT security practices in a less standardized way. For instance, a hospital's data breach risks might not be lower after adopting an advanced application to scan for security vulnerabilities without sufficient patching capabilities.

In the analysis, we measure IT security capability by using the mean yearly value of all adopted IT security applications *before* a hospital joins HIE. First, we only consider hospitals that join HIE from 2013 onwards, so we can observe at least one year IT security investment before joining HIE. Second, we measure the IT security capability using the annual average of prior IT security investment. The main reason is that hospitals join HIE in different years. For example, if hospital A adopts four, five, and six IT security applications in 2010, 2011 and 2012 before joining an HIE in 2013, its prior IT security investment is measured as five. If hospital B joined an HIE in 2015, its IT security capability is the average number of IT security applications from 2010 to 2014.¹⁷ There are two main advantages of the measurements. First, the

¹⁷If the numbers of adopted IT security applications in hospital B from 2010 to 2014 are 3 (2010), 4 (2011), 5 (2012), 6 (2013), 6 (2014), its IT security capability is $(3 + 4 + 5 + 6 + 6)/5 = 4.8$.

proxy is an accumulated variable. Hence, it can better represent the stock knowledge and experience in implementing data security protection. Second, the proxy is solely based on pre-treated variables and is free from HIE’s impact, thereby mitigating the concern of “bad control” issues (Cinelli et al. 2020). The rationale is that a hospital’s IT security capability is relatively stable across different years before joining HIE.

$$ITSecurityCapability_i = \frac{\sum_i^{j-1} ITSecurityInvestment_i}{j - i}$$

i : Start year (2010 in our data); j : Join in an HIE at year j

To examine the moderating role of IT security capability, we incorporate the interaction term $JoinHIE_{it} * ITSecurityCapability_i$ in the main model specifications. In our setting, $ITSecurityCapability_i$ is a control variable since it is a time-invariant variable and is absorbed by hospital fixed-effects. Column (1) of Table 6 shows that an HIE hospital experience a larger magnitude of reduction in breach likelihoods if it has a higher IT security capability. Figure 2.2 explicitly illustrates how the effect of HIE differs by hospitals’ IT security capabilities. To further test the result, we use an alternative measurement that only counts the accumulated number of IT security applications between 2010 to 2012 since most hospitals joined HIEs in 2013 and onwards. The results are reported in Column (2) of Table 6, which consistently show the significantly negative moderating effect of IT security capability.

The result supports our assertion that hospitals with higher frictions in security protection (lower IT security capability) realize a smaller magnitude of reduction in data breach likelihoods. Moreover, the coefficient of Join HIE is positive, suggesting that hospitals with sufficiently low IT security capability may experience higher data breach risks after joining an HIE. The results provide suggestive evidence for the existence of security risks when joining an HIE.

Table 2.6. Heterogeneity Analysis: Hospital's IT Security Capability

	(1)	(2)
DV: Data Breach Occurrence	IT Security Capability	Alternative Measurement
Join HIE	0.033* (0.015)	0.024 (0.017)
Join HIE* IT Security Capability	-0.013** (0.004)	-0.011* (0.005)
R-squared	0.294	0.290
Observations	9176	9130
No. Hospitals	1637	1600
Hospital & Year FE	YES	YES
Control Variables	YES	YES

Notes: All estimations use cluster-adjusted robust standard errors (clustered at the hospital level).

We use a matched sample in these analyses. *** $p < 0.001$, ** $p < 0.01$, * $p < 0.05$, + $p < 0.1$

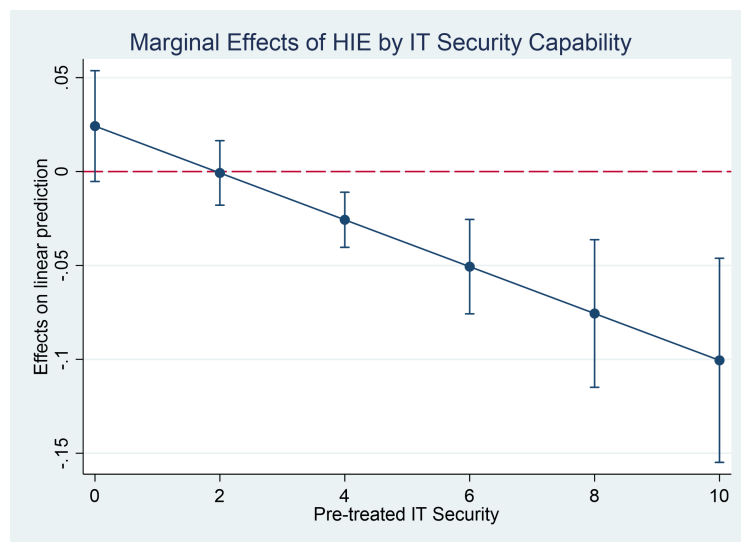


Figure 2.2. The Marginal Effect of HIE on A Hospital's Data Breach Likelihood by its IT Security Capability

2.7.4 HIE Security Laws

A hospital is more likely to achieve better security performance after joining an HIE when the effectiveness of the governance is high (*Lemma 3b* in the theoretical framework). Although it is difficult to directly measure the effectiveness of the HIE governance, we leverage an external law shock to indirectly measure this construct. The main intuition is that although the HIE governance is based on mutual benefits among organizations, it is still possible that its effect on data breach risks is sub-optimal, and related regulations' enactments may improve the effectiveness of HIE governance on data security protection.

State-level HIE security laws aim to impose more accountabilities of data security on HIEs and specific data exchange standards. For example, New Hampshire enacted HIE security laws on September 9, 2014 (N.H. Rev. Stat. § 332-I:10). It requires HIEs to “implement recognized national standards for interoperability and transmission security. Transmission security standards shall guard against unauthorized access to electronic health information that is being transmitted over an electronic communications network and shall include appropriate integrity controls and encryption mechanisms following HIPAA security regulations.”

To compile a completed list of state HIE security laws, we collect data from the The Office of the National Coordinator (ONC)'s State Health IT Policy Levers Compendium¹⁸ and Health Privacy Project at Georgetown University.¹⁹ These websites collect state privacy and security policies on Health IT. To make sure that these laws cover HIEs, we follow practices in Schmit et al. (2017) and manually search keywords (e.g., “HIE” “Security” “Breach” etc.) in the Westlaw legal database. Furthermore, we code laws as state-level HIE security law only when they address specific safeguards to secure HIE data and do not refer to state or federal laws. In our analysis, a dummy variable `HIESecurityLaws` is one of the states with the law in a specific year; otherwise, the value would be zero. Results in Table 7 show the significantly negative

Table 2.7. Heterogeneity Analysis: HIE Security Law

DV: Data Breach	HIE Security Laws
Join HIE	-0.009 (0.009)
Join HIE* State HIE Security Laws	-0.025* (0.011)
State HIE Security Laws	0.003 (0.008)
R-squared	0.287
Observations	9387
No. Hospitals	1644
Hospital & Year FE	YES
Control Variable	YES

Notes: All estimations use cluster-adjusted robust standard errors (clustered at the hospital level). We use a matched sample in these analyses. *** $p < 0.001$, ** $p < 0.01$, * $p < 0.05$, + $p < 0.1$

coefficients of the interaction term. They suggest that HIE security laws can enhance HIE governance's effectiveness, further reducing hospitals' security breach risks.

2.8 Robustness Checks

2.8.1 Endogeneity and Identification Strategies

In an ideal experiment, hospitals would be randomly assigned to join HIEs. However, this is impossible in a practical setting considering the high cost. Therefore, our observational study may experience biases from three sources: confounding factors,

¹⁸<https://dashboard.healthit.gov/apps/state-health-it-policy-levers-compendium.php>

¹⁹<http://www.healthinfolaw.org/>

reverse causality, and selection bias. We approach each of these with additional tests and robustness analyses as follows.

First, confounding factors can simultaneously affect hospitals' data breach risks and their tendency to join an HIE. For example, if more patients visit a hospital, a breach incident may increase losses. Hence, the focal hospital may be motivated to enhance its data security protection. At the same time, the propensity of joining an HIE would also become higher since the hospital needs historical diagnosis information on their patients from different sources to improve its service quality. To deal with the concern, we use two-way fixed effects and leverage a set of hospital and hospital referral region characteristics to capture time-variant shocks. Additionally, we use a matching approach to select a sub-sample of hospitals that share similar characteristics, after which a difference-in-differences estimation is used to isolate the impact of joining an HIE. In that case, we can perform analyses on a more balanced sample, and the results are less likely to be affected by systematic differences (Dehejia and Wahba 2002). Combining matching with DiD is widely used as an identification method in IS literature (Greenwood and Wattal 2017, Sun et al. 2020). We also conduct robustness checks, including using instrumental variables (2.8.3) and incorporating state-year specific trends (Table A.2) to ensure the results are robust.

Second, reverse causality poses a concern. For instance, hospitals with better security posture may be more likely to join HIEs. It is possible that that hospital administrators perceive that they can learn more about security practices after joining HIE. To deal with the potential reverse causality, we use different relative-time models that incorporate lead and lagged HIE participation indicators in Section 2.8.2. The results show no significantly decreasing trend in breach risks before hospitals join HIEs.

Third, selection bias may be a concern with our data. On the one hand, one can argue that HIEs select their participants based on their IT profiles and security postures. However, this rarely happens in the real world. In most cases, HIEs are incentivized to attract more healthcare providers to join their sharing networks to increase their value (Demirezen et al. 2016). As a result, they are unlikely to select

the participants based on their IT security performances. Also, it is challenging to predict future security breaches considering the complexity of causes. On the other hand, one can also argue that hospitals' decision to join HIEs can lead to self-selection issues. If hospitals that value data security are more likely to join HIEs, the impact of HIEs on breach probability is likely to be spurious. However, previous studies suggest that the concern about increasing security risks in data sharing is a significant barrier in joining HIEs (Adler-Milstein et al. 2011). In other words, hospitals that value data security less are more likely to join HIEs, which makes our results more conservative when the associations between HIEs participation and data breaches are negative.

Additionally, we also perform other robustness tests such as performing Bacon decomposition and using alternative models. Table 2.8 summarizes the main concerns in analyses and related robustness checks.

Table 2.8. Summary of Robustness Tests

Concerns	Tests	Findings	Locations
Reverse causality	Relative-time model	No pre-treated trend and results remain consistent	Table 2.9
Omitted variables	Instrument Variable	Results remain consistent	Table 2.10
The time-varying treatment effect is invalid	Bacon decomposition	Results remain consistent	Table 2.11
State-level policy confounds the main impact	State-specific trends	Results remain consistent	Table A.2
Results are sensitive to model specification	Non-linear models	Results remain consistent	Table A.3

2.8.2 Relative Time Models

The parallel trend assumption is critical to the validity of DiD estimation. In our context, it is necessary to test whether hospitals in the treated group (i.e., join HIE) have lower data breach risks even before joining HIE. Therefore, we use relative time models to examine pre-treated trends. Like previous practices (Adjerid et al. 2018, Chan and Ghose 2014), we incorporate relative time dummies to indicate the relative yearly sequential distance between an observation year, t , and the year when a hospital joins an HIE, i . In the analyses, we remove hospitals in HIE at the start of our data collection period (2010) because we cannot infer the exact year that they join HIE. Therefore, we lose 25% of observations in estimating relative time models.

We report estimated effects of bivariate and multivariate models along with relative-time models in Table 2.9. The results demonstrate that hospitals that join HIE experience a statistically significant decrease in data breach risks. Columns (1) and (2) present that a hospital's data breach probability decreases after joining an HIE. Importantly, the coefficients of $JoinHIE_{t-3}$ and $JoinHIE_{t-2}$ are insignificant, providing evidence that there are no pre-treated trends.

Table 2.9. Relative-time Model

DV: Data Breach Occurrence	(1) Benchmark	(2) Control Variables
T - 3	-0.006 (0.008)	-0.009 (0.008)
T - 2	-0.009 (0.009)	-0.014 (0.009)
T - 1	(Omitted)	(Omitted)
T = 0	-0.019* (0.010)	-0.022* (0.010)
T + 1	-0.018+ (0.010)	-0.024* (0.010)
T + 2	-0.053*** (0.013)	-0.055*** (0.014)
R-squared	0.264	0.271
Observations	14344	13090
No. Hospitals	2400	2310
Hospital & Year FE	YES	YES
Control Variables	0.264	0.271

Notes: All estimations use cluster-adjusted robust standard errors (clustered at the hospital level).
 *** p<0.001, ** p<0.01, * p<0.05, +p<0.1

2.8.3 Instrumental Variables

We employ Instrumental Variables (IVs) and Two-Stage Least Square estimation to test our results further. Similar to previous studies (Miller and Tucker 2009, Angrist and Pischke 2008), we use a linear probability model with IVs that performs similarly to some non-linear model specifications (Angrist and Krueger 2001). In our context, there are two main identifying assumptions. First, these instruments are sufficiently associated with focal hospitals' tendency to join HIEs. Second, they do not directly change hospitals' data breach risks conditional on necessary hospital-level and HRR-level covariates. We choose three regional-level instruments and provide justifications for these assumptions.

The first instrument is the percentage of hospitals joining HIEs in hospital referral regions (HRR). The rationales are three-fold. First, the HIE participation ratio can

capture regional level incentives that motivate hospitals to join HIEs (Ross et al. 2010, Rudin et al. 2014). Second, the network effect is evident in HIEs (Demirezen et al. 2016, Miller and Tucker 2014). The more hospitals that join HIEs, the more valuable the HIE would be. Therefore, the higher the percentage of participation, the more likely the focal hospital will join HIEs. Third, the instrument also represents the normative pressure, facilitating HIE participation (Hsu et al. 2012, Robey et al. 2008). Hence, the ratio should be positively associated with a hospital's likelihood of joining in HIEs. Also, it may not directly affect focal hospitals' breach risks.

The second instrument is the number of health systems in hospital referral regions. According to The National Bureau of Economic Research (NBER) Center of Excellence's definition, a health system consists of two or more healthcare provider organizations that have common ownership or cooperate closely (AHRQ 2017). Some well-known health systems include Mayo Clinic, HealthOne, Allina Health, etc. A hospital in an HRR with more unique health systems is less likely to join HIE. The main reason is that system fragmentation in the local healthcare market is positively associated with HIE organizations' coordination costs. Because of disparate practices and policies, it takes more time and effort to establish data exchanging processes when a region has more unique health systems. Furthermore, different health systems are likely to adopt health IT from different vendors, making it more challenging to achieve interoperability (Everson and Adler-Milstein 2016). Again, the instrument would not affect hospitals' data breach risks conditional on a set of hospital-level and HRR-level control variables.

The last instrument is state-level HIE laws. A few states, including Minnesota, Texas, Kentucky, Pennsylvania, and Vermont enacted policies to guide HIE accreditation, certification, registration, or qualification.²⁰ These policies increase HIE legitimacy, incentivizing hospitals to join HIEs. Since the policies were designed and enforced by state governors, it is unlikely that they would affect individual hospitals' breach risks through other channels rather than HIE participation. Therefore, it is a valid instrument in our context.

²⁰<https://www.healthit.gov/data/apps/state-health-it-policy-levers-compedium>

Table 2.10 presents the results of IV estimation. Consistent with the theories discussed above, in Column (1), the coefficients of three IVs are consistent with theories. Furthermore, results in the second stage prove the validity of our instruments. First, the three IVs are not weak. The Kleibergen-Paap rk Wald F statistic is more than 300, which is much larger than the rule of thumb value of 10 (Staiger and Stock 1997), allowing us to reject the null hypothesis of weak instruments. Second, all Hansen J p-values are larger than 0.1, showing our IVs meet the exclusion restriction. Notably, the results are consistent with the previous findings.

Table 2.10. Instrument Variables – 2SLS Estimations

Outcome	(1)	(2)	(3)	(4)
	Stage 1: Join HIE	Stage 2: Data Breach Occurrence		
State HIE Certificate	0.017 (0.015)			
HRR HIE Participation	0.958*** (0.033)			
No. Health Systems in HRR	-0.007 (0.006)			
Join HIE		-0.069*** (0.017)	0.059* (0.027)	-0.062*** (0.018)
JoinHIE * IT Security Capability			-0.030*** (0.007)	
JoinHIE * HIE Security Laws				-0.021* (0.010)
Observations	18129	18129	11591	18129
No. Hospitals	3210	3210	2081	3210
Hospital & Year FE	YES	YES	YES	YES
Control Variables	YES	YES	YES	YES
Significance of first-state regressions		412	377	412
Hansen J p-value		.502	.684	.153

Notes: All estimations use cluster-adjusted robust standard errors (clustered at the hospital level). In Column (2) (or (3)), we follow common practices and use interaction terms of two instruments and ITSecurityCapability (or HIESecurityLaws) as new instruments. *** $p < 0.001$, ** $p < 0.01$, * $p < 0.05$, + $p < 0.1$

2.8.4 Time-varying Treatment Effects

Recent methodology papers point out the potential issue in time-varying treatment DiDs with two-way fixed effects (Baker et al. 2021, Callaway and Sant’Anna 2020, Goodman-Bacon 2021). Two-way fixed effects model estimator is the weighted average of all possible 2X2 DiD estimators. The fact that treatment effects may vary

across time may bias the estimates. Specifically, units in timing groups, who are being treated at different times, can serve as each other’s such as *Later Adopters* (as treated) and *Early Adopters* (as control). The comparison is likely to bias the result or even the direction of the true effect if the treatment effect is heterogeneous (Baker et al. 2021).

To test the validity of our DiD, we use Bacon decomposition to identify the weights of the estimated effect (Goodman-Bacon 2021). The results in Table 2.11 and Figure 2.3 present several main comparisons, including Timing groups, Always vs Timing groups, Never vs Timing groups, and Always vs Never groups.²¹ Three main findings pertain to the appropriateness of our estimated treatment effect. First, more than 50% of estimated treatment effects stem from “Never vs. Timing Group,” which is a reasonable comparison between treated units (Timing) with control units (Never). Second, the magnitude of “Never vs. Timing Group” treatment effect is similar to the average treatment effect in our main model. Third, the weight of “Timing groups” is fairly low (7%), which suggests that it cannot substantially bias our results. To summarize, these results alleviate the concern that the DiD estimate is biased in our setting.

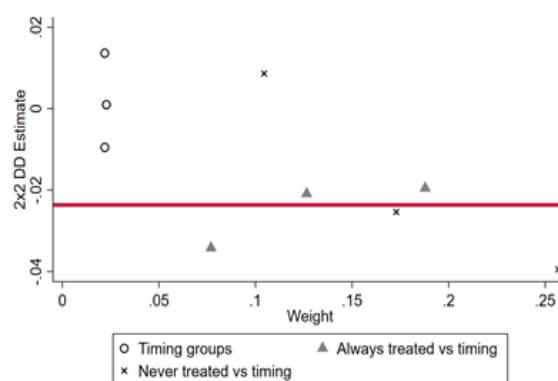


Figure 2.3. Bacon Decomposition Results

²¹ “Within” is a residual component.

Table 2.11. Bacon Decomposition Results

Groups	Coeff.	Weight
Timing groups	0.00	0.067
Always vs Timing	-0.02	0.391
Never vs Timing	-0.03	0.534
Always vs Never	-2.29	0.000
Within	-0.13	0.007

2.8.5 Other Sensitivity Tests

We perform a series of diagnostics and robustness checks to examine the sensitivity of our primary findings in response to some major empirical concerns. First, it is possible that state-level policies regarding information security or health information technology may confound HIE’s impact. Therefore, we incorporate state-year-specific trends to capture all state-level shocks, and our results remain robust. The results are presented in Table A.2 in Appendix.

We also test whether we can obtain similar results from nonlinear models. Since the outcome variable is binary, we use Probit models to estimate the above analyses. Our results are consistent with our previous findings. We report the results in Table A.3 in Appendix.

2.9 Additional Analyses

2.9.1 Breaches of Different Locations

We examine each incident’s description and label it based on breached locations (IT system or physical). For example, in hospital A, an employee accessed 1,997 patients’ data in Electronic Medical Record (EMR) systems to commit insurance fraud. As this type of breach occurred in the EMR system, this incident belongs to

the “IT systems” (location) categories. In hospital B, a doctor’s laptop computer was stolen, and the missing laptop contained protected health information for more than 800 patients. We label the incident as a “physical breach” (location). We summarize detailed definitions of each type in Table 2.12.

Table 2.12. Definitions of Breach Locations

Breach Type	Definitions
IT system breach	Breached locations are electronic systems. e.g., EMR breaches, network, web servers.
Physical breach	Breach locations are physical entities. e.g., Equipment loss (including desktop, laptop, portable devices loss) and paper loss.

Next, we use a binary indicator to represent the occurrence of each type of breach incident. Then, we examine how the treatment affects different types of breaches by regressing the focal variable on the indicator of breach categories. The results in Columns (1) of Table 2.13 show reductions of 1.7 percentage points in the likelihood of IT system breaches after the focal hospital joins in an HIE. However, Columns (2) suggest that joining HIE has an insignificant impact on physical breaches.

Table 2.13. Different Types of Breaches: Locations

Outcome	(1) IT System Breach	(2) Physical Breach
Join HIE	-0.017** (0.006)	-0.004 (0.007)
R-squared	0.219	0.292
Observations	9387	9387
No. Hospitals	1644	1644
Hospital & Year FE	YES	YES
Control Variables	YES	YES

Notes: All estimations use cluster-adjusted robust standard errors (clustered at the hospital level). We use a matched sample in these analyses. *** p<0.001, ** p<0.01, * p<0.05, +p<0.1

The significant reduction in IT system breaches might be attributed to system integrations in hospitals after joining HIEs. Specifically, governance can protect electronic data sharing links that are connected to IT systems such as Electronic Health Record systems, network systems, and servers. Also, interoperability requires disparate systems to follow the same protocols at certain levels, ensuring that hospitals comply with similar security standards and practices to reduce IT system breaches. HIE governance can also detect abnormalities in electronic data sharing channels and adopt preventive approaches to mitigate potential risks. In contrast, it is more challenging for HIE governance to monitor and control potential risks in most physical settings.

2.9.2 Breaches of Different Threat Actors

We explore how joining HIE affect hospitals' breaches that are caused by different types of threat actors, including hackers, malicious insider, and unintended disclosure. We use the instances of three types of breaches as the outcome variables. The results are in Table 2.14. Interestingly, while the likelihood of hacker breach occurrence significantly decreases, internal breach risks do not change significantly. There are two underlying reasons. First, the technical standard that is being applied in hospitals, which are more effective in deterring hackers' attacks. Second, HIE usage may interrupt internal employees' workflow, offsetting the impact of increased protection in response to HIE participation.

Table 2.14. Different Types of Breaches: Threat Actors

Outcome Variable	(1) Hacker Attack	(2) Insider Breach	(3) Unintended Disclosure
Join HIE	-0.012* (0.005)	0.001 (0.004)	-0.005 (0.006)
Constant	-0.311 (0.503)	-0.003 (0.242)	0.932* (0.463)
R-squared	0.215	0.221	0.306
Observations	9387	9387	9387
No. Hospitals	1644	1644	1644
Hospital & Year FE	YES	YES	YES
Control Variables	YES	YES	YES

Notes: All estimations use cluster-adjusted robust standard errors (clustered at the hospital level).

We use a matched sample in these analyses. *** $p < 0.001$, ** $p < 0.01$, * $p < 0.05$, + $p < 0.1$

2.10 Discussion

2.10.1 Main Findings

This study's main objective is to investigate how sharing electronic health data via Health Information Exchanges (HIEs) affects hospitals' data breach risks. The public and healthcare providers alike have expressed concern that data security risks become higher when hospitals start to exchange data across their boundaries as the interdependence and data access increase. However, we identify another possibility – that HIE governance can effectively lower these risks by enhancing IT security protections. We explore the tension between increased security risk and HIE governance by using an analytical model to show that a hospital's security breach likelihood can increase or decrease depending on the effectiveness of HIE governance. Furthermore, hospitals increase their IT security investment when HIE governance becomes more effective. Besides, the improvement of data security is of larger magnitude in hospi-

tals with a lower unit cost of protection or when the effectiveness of HIE governance increases.

To test these insights from our theoretical model, we use an empirical model to examine HIE participation's effect on hospitals' data breach risks. The findings show that after joining an HIE, hospitals' data breach risks decrease. In a further step, we find that hospitals adopt more IT security applications, while their IT security capability affects the magnitude of reductions in breach risks. Besides, external enforcement of HIE security laws can enhance the reduction in HIE hospitals' breach risks. The results are robust to considerations of omitted variables, reverse causality, and self-selection. Additionally, we find that the likelihoods of experiencing IT system breaches and hacking incidents significantly decrease after a hospital joins an HIE. However, there are no significant changes in the likelihood of physical breaches or internal breaches.

2.10.2 Implications for Research

This study contributes to three main streams of literature in the IS field. First, we extend the information security literature in the inter-organizational system context. Most studies on organizational information security performances focus on one of two aspects: internal management and external security policies (Angst et al. 2017, D'Arcy et al. 2020, Hui et al. 2017, Kwon and Johnson 2014, Romanosky et al. 2011). The impact of general data sharing through IOS is much more nuanced. Most existing studies use analytical models to explore the topic (Fang et al. 2014, Huang et al. 2014). A few studies empirically examine the security dynamics in cross organizational scenarios in recent years, but the results are mixed (Baskerville et al. 2018, Tanriverdi et al. 2019). Our study is the first to investigate realized changes in security risks after hospitals start to share data electronically across organizational boundaries. Furthermore, we investigate the main mechanisms by examining the heterogeneity of HIE's impact.

The study also contributes to the IOS literature. Previous studies in this field associated IOS with various benefits within technical, organizational, and political spheres (Dawes 1996, Gil-Garcia and Sayogo 2016). Nevertheless, security risks, regarded as major conflicts in IOS (Kumar and Dissel 1996), are seldom examined. Also, IOS governance is needed to address the conflicts (Chatterjee and T.Ravichandran 2013), leading to interesting dynamics in the realized outcomes. Nevertheless, we are not aware of any empirical study quantifying the impact of IOS adoption on security risks. Our findings illustrate the unexpected effects of breaking information silos among organizations' coordination in the information security field.

Third, this study contributes to the health IT literature. HIEs, as large-scale health IT initiatives in the United States, enable data sharing among disparate health-care providers and improve healthcare efficiency in many aspects (Adjerid et al. 2018, Atasoy et al. 2017, Ayabakan et al. 2017). However, security risks have always been regarded as the main obstacles in HIE adoptions. Our results provide evidence that governance in HIEs facilitates coordination in the cybersecurity landscape, which improves overall security performance in hospitals. The findings complement previous studies on health IT and hospitals' security postures (Kim and Kwon 2019, Miller and Tucker 2011). Furthermore, the study suggests that HIE is more than providing a channel for hospitals to exchange medical information and knowledge. The governance in the process is critical in mitigating risks, which is worthy of further investigation. Additionally, our results reveal that reductions in data security risks are of larger magnitudes on hospitals with higher prior IT security capability, emphasizing the importance of cybersecurity maturity before establishing interoperability among hospitals.

2.10.3 Implications for Practice

Our study offers several implications for practitioners and policymakers. First, it is essential for different stakeholders to realize how connecting to HIEs impacts the adopting hospitals' security postures, given the increasing prominence of privacy and

security in data sharing. To establish a more active health data sharing network, policy-makers and HIE administrators should emphasize policies and practices that can mitigate concerns raised by the public. Greater data protection efforts can enhance trust between different parties, facilitating collaborations and promoting data interoperability. Furthermore, our analytical model illustrates the possibility of an increase in security risks when data starts to flow. In other words, the improvement in security posture will only be realized when hospitals can effectively protect data at a lower cost, and the likelihood of shared risks is relatively low.

Organizations' IT security capability plays a critical role in realizing the improvement in data security. Though the hospitals' data security performance improves after joining an HIE, the magnitude of improvement is smaller for hospitals with low IT security capability. This finding is particularly important considering the risks can involve other participants in the same HIE network. Therefore, policy-makers and HIE administrators must identify those hospitals and provide more assistance to improve their security posture. For example, HIE can offer training or subsidies to help member hospitals that experience difficulties in digital transformations and data protection. A few HIEs have already started to offer IT security services, which may prove mutually beneficial.

Third, HIE governance effectively reduces IT system breaches and hacking breaches. On the contrary, its impacts on physical and internal breaches are insignificant. To effectively lower the risks of physical breaches and internal breaches, it is necessary for policymakers, HIE administrators, and hospitals to develop new collaborative patterns. In particular, physical data security should not be ignored since more devices have started to store patient data. When these devices are compromised, malicious attackers may gain illegal access to large amounts of data (e.g., a laptop containing unencrypted data is stolen). Therefore, HIEs can consider promoting effective camera surveillance to reduce the likelihood of physical breaches. Also, HIE can promote workflow improvement, conduct employee security training, and increase audit frequency to lower internal breaches. These practices should be considered in designing and establishing IOS security frameworks.

Additionally, given an increasing number of breach incidents caused by third parties, more practitioners realize the importance of “risks across walls” (risks across organizational boundary). However, cross-organizational data governance is not well understood. Our study suggests that the HIE model could be a useful reference for other IOSs to reduce risks. Although IOSs are different in technical infrastructures, complexity, and openness, the core is to bridge data sharing among organizations. Managers and chief information security officers (CISO) need to establish a practical governance framework to control risks over the networks. Furthermore, assessing participants’ security risks is critical before sharing data. The third-party risk assessment business’s prevalence also reveals that data security posture has already become a key metric when evaluating collaborators.

2.10.4 Limitations and Future Directions

This study is subject to a few limitations. First, the measurements we use have limitations. For instance, we use a binary indicator to show hospitals’ HIE status for the treatment variable. A lack of HIE-level data makes it challenging to capture finer grain mechanisms. Future studies can investigate how variations in HIEs’ organizational, governance, and technical structure affect the overall data breach risks. Furthermore, we only use proxies in analyses, such as hospitals’ IT security capabilities. It would be helpful to collect more detailed data on security investment (security training, security employees) to develop more precise measurements. Additionally, our outcome variable cannot tell us whether breach incidents involve multiple hospitals’ health records. It would be interesting to measure the cost and benefit of joining HIEs more precisely if the data are available.

Second, similar to many observational studies, endogeneity is a major concern in our research. Although we deal with these issues using a set of identification strategies to carefully exclude the confounding impacts and address the reverse causality and selection bias, full causality cannot be established using secondary data such as ours.

Third, this study relies on the healthcare context where data security is highly valued and regulated by HIPAA, HHS data breach notifications, and state laws. For other industries where the institution does not have stringent regulations for data protection, the IOS adoption may increase data breach risks. However, according to our analytical models and empirical results, our results can still inform IOS in a different industry from two main perspectives. First, organizations should have enough experience in IT security performance; otherwise, their security performance may not be improved. Second, IOS governance should be effective in reducing shared risks. If not, organizations may not have substantial incentives to enhance their data protection. Considering the limited number of studies on security data sharing across organizational boundaries, we call for related research in other settings. There are still many new and interesting questions around the IOS and information security, and they could be directions for future research.

CHAPTER 3

HOW TO MAKE MY BUG BOUNTY COST-EFFECTIVE? A GAME-THEORETICAL MODEL

Abstract

To mitigate the threats from malicious exploitation of vulnerabilities, an increasing number of organizations across different industries have started incorporating bug bounty programs (BBPs) in their vulnerability management cycles. A bug bounty program (BBP) attracts a crowd of external security researchers to search for new vulnerabilities in the IT systems. For organizations that launching the crowdsourcing cybersecurity solution, one key question is: How to design the incentive and improve the cost-effectiveness of an BBP as a layer of vulnerability management? However, this problem has not been analyzed in the literature. To fill this important gap, we use a game-theoretical model to examine several related research questions where we consider the characteristics of (i) the organization's security posture and patching complexity, (ii) security researchers' efficiency and number, and (iii) the level of legal protection for security researchers. The findings reveal that organizations need to be strategic in designing bounties when its patching complexity is high. However, organizational security postures can substitute for bounties. Furthermore, having more efficient or a larger number of security researchers may not necessarily implies an increased bounty and lower total costs. A bounty's public relation effect plays a critical role in deciding the changes. Lastly, when there is an increased level of legal protection for security researchers, an organization may increase the bounty size and experience lower total costs. This study provides several insights to security professionals, organizations, and policymakers in designing effective bug bounty programs.

3.1 Introduction

Worldwide spending on information security has increased significantly in recent years and is expected to surpass \$170.4 billion in 2022 (Morgan 2019). In confronting higher information technology (IT) security risks and more stringent regulations in protecting digital information, organizations across different sectors are seeking new cybersecurity solutions to improve their security performance strategically (Help Net Security 2019). Many of them have started tapping into the security researcher community and collecting vulnerability information with bug bounty programs (BBPs) (Statista 2021). In 2018, the National Institute of Standards and Technology's (NIST) cybersecurity framework was updated and now recommends that companies need to consider establishing processes to receive and deal with vulnerabilities submitted from external sources including security researchers (Ellis 2021).

Similar to most crowdsourcing programs, a BBP is helpful in gaining attention and collecting innovative outputs from a group of external participants (Finifter et al. 2013). Specifically, security researchers can report undiscovered vulnerabilities in organizations' IT infrastructure or digital products. After receiving the reports, organizations can patch these vulnerabilities to mitigate potential losses in cyber attacks. As a result, BBPs are regarded as helpful in improving organizations' IT security performance (Alomar et al. 2020, Malladi and Subramanian 2019). However, BBPs are part of the enterprise vulnerability management, which makes them substantially different from other crowdsourcing tasks. In particular, from the perspective of enterprise security management, how to better incorporate a BBP as a layer of security control is a critical question that hasn't been examined sufficiently.

This question becomes especially important to organizations across almost every industry due to the growing dependence on IT. BBPs have become prevalent as many organizations are launching their own programs. An increasing number of organizations in both private and public sectors have been recognizing the values of BBPs, including government agencies like the U.S. Department of Defense (Marks 2018, Wroten 2020). Prominent IT firms such as Facebook, Google, and Apple also

have their own BBPs.¹ Furthermore, some organizations have turned to BBPs when there were public concerns about their security performance. For example, Zoom has announced to make improvements in its BBP after facing doubts and criticism about security issues (Cimpanu 2020).

Although crowdsourcing security solutions have gained popularity in practice (Broshevan 2019), there is a dearth of formal analysis examining how to design the award and how to improve the cost-effectiveness of a BBP considering the security features of an organization (Cassin 2020, Marino 2020), the characteristics of security researchers (Brown and Minor 2014, Boudreau et al. 2011), the level of legal protection offered to the participants (Park and Albert 2020, Haworth 2021), and the public relations (PR) effect of BBPs (Terrill 2018, Osborne 2022). We fill these gaps in the literature by formally investigating how the bounty and the performance of the BBP are impacted by the characteristics of the security researcher community, characteristics of the organization, and the legal underpinnings of the BBP. Furthermore, we provide practical implications for organizations, IT security professionals, and policymakers.

3.1.1 Motivation

A BBP is a layer of the enterprise vulnerability management paradigm, which makes it substantially different from other crowdsourcing tasks (Pratt 2022). In effect, managing a BBP is challenging because of several trade-offs (Bugcrowd 2017), involving various costs and benefits related to the vulnerability or the BBP (i.e., *expected damage cost*, *expected post-discovery cost*, the *bounty* itself). The trade-offs are affected by several important factors including (i) organization’s security characteristics (such as *patching complexity* and *security posture*), (ii) crowd’s characteristics (such as *productivity*, *heterogeneity*, and *group size*), and (iii) *legal uncertainties*. We elaborate on each of these factors as follows.

¹<https://www.facebook.com/whitehat;> <https://developer.apple.com/security-bounty;>
[https://www.google.com/about/appsecurity/reward-program/.](https://www.google.com/about/appsecurity/reward-program/)

To help them analyze security issues in their IT applications or infrastructures, by establishing a BBP, organizations can encourage security researchers that work independently and present heterogeneity in terms of their skills or productivity (Finifter et al. 2013). Therefore, the BBPs may strengthen organizations' security profiles since the "wisdom of crowd" can compete with the rate at which the inherent vulnerabilities of the software are abused (Anderson and Moore 2006). If the vulnerabilities were exploited before a fix is developed, the consequences can be serious (Bloomberg 2018). For example, the Equifax's 2017 data breach was due to the exploitation of an unpatched vulnerability in the consumer complaint web portal (Fruhlinger 2020). This breach has been deemed as "entirely preventable" by simply discovering and patching the vulnerability in a timely manner (Whittaker 2018). Discovering vulnerabilities, then, is even more critical for organizations with limited cybersecurity expertise. With the help of security researchers in BBPs, a vulnerability might have been identified, and hence, fixed earlier (i.e, the lifecycle of the vulnerability decreases). Therefore, BBPs can lower such *expected damage costs*. In addition to motivating security researchers, a bounty has a collateral benefit on reducing the damage cost based on a public relation (PR) effect (Hata et al. 2017). Unlike other security investments, announcing a bounty usually attracts media attention especially when the amount of the bounty is high (Cimpanu 2020). Since a BBP shows the engagement with the security community, it advocates that the organization highly values security (Terrill 2018). Therefore, a bounty can offset the "perceived" damage cost partially in addition to its main impact in identifying the vulnerability earlier.

Nevertheless, offering a higher bounty has cost implications beyond the cost of the bounty per se. By designing a BBP, the organization actually increases the overall search effort among the participating security researchers (Zhao et al. 2016). As a result, such an increased level of scrutiny in the search efforts may also result in leaks out of the program (Crews et al. 2018). These leaks do not have to be in the form of actual submissions or the proof of concept (showing how the vulnerability can be exploited) as any information or any hint about a tool can turn out to be disastrous

for the organization (Nidecki 2020). Therefore, this *expected post-discovery cost* is one of the important considerations of the organizations that run BBPs.

An organization's security characteristics impact the performance of its BBPs. Unlike most crowdsourcing programs, a BBP is a layer of enterprise vulnerability management in which an organization's timely response and remediation are critical (Ransbotham and Ramsey 2012, August and Tunca 2006). Therefore, the organization's security features are an important contributor to the success of BBPs. In particular, two key features are critical in affecting BBPs: patching complexity and security posture. Patching complexity is influenced by the IT system or infrastructure of the organization and represents the complexity of remediating discovered vulnerabilities. For instance, patching vulnerabilities in core IT systems is more complex since they create a longer downtime or operational problems (Shein 2022). Since patching complexity determines the baseline of patching time, it substantially affects BBP's payoffs. Another critical feature is an organization's security posture which represents the established capability in IT security control (NIST 2014). A high level of security posture is generally a long-term endeavor that requires consistent security investment and training (Petersen 2019). Therefore, this metric represents the overall security capability and affects the organization's efficacy in dealing with vulnerabilities. Along with the patching complexity, the security posture determines the realized patching duration, and further impacts various costs (such as the damage cost and the post-discovery cost that are discussed earlier), thereby influencing the BBP's performance. Therefore, assessing and examining the roles of organizational security features in BBPs has non-trivial implications.

In crowdsourcing (resp., a BBP), the participants are, in a way, competing to make an innovation (resp., discover a vulnerability) first. Hence, to organizations, the productivity and the total number of participants are critical in determining the performance of crowdsourcing programs (Ales et al. 2019). These crowd-based characteristics are also critical in BBPs. First, the productivity of security researchers can directly affect the outcomes of BBPs. Furthermore, security researchers are not homogeneous regarding their productivities since BBPs usually attract security

researchers with various backgrounds and skill sets (Al-banna et al. 2018, Hata et al. 2017). Although this heterogeneity is being debated in practice, there is limited understanding regarding how it impacts the performance of BBPs (e.g., see Zhao et al. 2017). Lastly, the number of participating security researchers in BBPs also plays an important role. As Linu’s Law claims, “given enough eyeballs, all bugs are shallow” (Raymond 1999, p. 1). Therefore, organizations need to carefully examine how security researchers’ characteristics affect their BBPs.

The legal underpinnings of BBPs also impact the dynamics of the BBP. In practice, the legal tensions between security researchers and organizations are salient in the context of BBPs (e.g., see Gamero-Garrido et al. 2017). Searching for vulnerabilities generally requires security researchers to perform tasks that are intrusive in nature, such as unauthorized access and transmission of sensitive information. There are several occasions where seemingly usual security researchers have been regarded as illegal hacking activity and the security researchers could not get the promised bounty (e.g., see Zhang 2017). Therefore, some level of legal protection is necessary for security researchers to participate in BBPs. A higher level of legal protection motivates security researchers to exert more effort. On the other hand, a higher level of legal protection also gives an opportunity for security researchers to be more relaxed in their search processes. A higher level of legal protection then potentially amplifies the post-discovery costs that are due to possible leaks out of the program. Hence, the level of legal protection has been one of the hotly debated topics in practice and legislative bodies. For example, in May 2022, the U.S. Department of Justice announced revised the Computer Fraud and Abuse Act, which made it illegal to access IT systems without proper authorization, increasing the level of legal protection offered to “good faith” security researchers that are searching for vulnerabilities (Department of Justice 2022). Therefore, the level of legal protection set by the authorities is an important factor in the performance of BBPs.

In summary, we investigate the role of participation-side, organizational characteristics, and legal regimes on *the optimal bounty* and *the total cost* of BBPs. In the next section, we discuss our research questions and contributions in detail.

3.1.2 Research Questions and Contributions

Many security professionals advocate that organizations should be strategic in their BBPs (Bugcrowd 2021). Although BBPs have become more prevalent in practice, only a limited number of studies have examined BBPs from the perspective of cost-effectiveness. Furthermore, the role of BBPs in the vulnerability management paradigm has seldom been investigated. Our paper fills these gaps and sheds light on several related questions by utilizing a game-theoretical model to formally examine an organization's strategies and outcomes in a BBP. Next, we provide a brief overview of our research questions and contributions.

First, we examine the roles of organizations' security features, including patching complexity and security posture. These two features are critical for the performance of a BBP as a layer in the vulnerability management paradigm. In practice, organizations have various digital assets that have different levels of patching complexity which affects the base level of patching time. Specifically, the higher the complexity is, the more time it would take to remediate or patch the vulnerability. Furthermore, an organization's security posture can affect the realized patching time. This is because patching efficiency is positively associated with the overall IT security control capability (Souppaya and Scarfone 2022). Furthermore, security posture impacts the realized base level of damage cost. Having a good security posture implies that the IT security control is effective and it is able to reduce a larger magnitude of the damage cost. However, it is unclear how these security features affect the bounty. Therefore, we ask: *Does having a higher patching complexity or worse security posture correspond to a lower bounty?* Proposition 3.4.1 addresses this question. One may think that an organization with high patching complexity and low security posture should not provide a higher bounty since they cannot patch the vulnerability promptly to reduce post-discovery costs. However, our results reveal that this is not necessarily the case.

Second, each security researcher participating in the BBP presents heterogeneity in their productivity or efficiency levels. This is critical for realizing the benefits of

BBPs (Sridhar and Ng 2021). Although there are some security researchers that can be regarded as experts, there are also some security novices that are significantly less productive and a whole spectrum of security researchers in between. Furthermore, increased levels of the lower bound (i.e., novices) and upper bound (i.e., experts) of productivity have opposite impacts on the heterogeneity among security researchers. Second, the number of security researchers is important to the vulnerability discovery process. Similarly, studies in economics extensively discuss how the number of participants in tournaments affects the overall performance of the tournament, and they suggest that a higher number of participants may increase or decrease the performance depending on contextual factors (i.e., see Boudreau et al. 2016).

Furthermore, in a BBP context, a higher number of participants increases the expected post-discovery cost. Therefore, it is not clear how the heterogeneity among security researchers and the number of them in the BBP impact the determination of the bounty itself and the total cost of the BBP. Therefore, we ask: *1. Does having a crowd of (a) security researchers of higher heterogeneity in productivity or (b) a larger size imply a higher bounty? 2. Does having a crowd of those characteristics correspond to a decreased total cost of a BBP?* Hence, we answer the question in Propositions 3.4.2 and 3.4.3. Interestingly, we find that an increased or decreased heterogeneity among the security researchers may or may not correspond to a higher bounty depending on the level of collateral benefits of bounties, i.e., the PR effect. Furthermore, having more productive experts is more beneficial to the organization in decreasing the total cost of the BBP. On the other hand, interestingly, having a larger crowd working on the bounty program may or may not be beneficial, and the answer depends on the current level of heterogeneity among the security researchers and, again, the PR effect.

Lastly, legal tensions in BBPs are salient due to the sensitivity of security vulnerabilities (Elazari 2018). To what extent can security researchers be protected under different regulatory regimes can substantially affect a BBP's payoff for organizations. This is because an organization may incur additional costs due to unintended violations or infractions in BBPs. To better understand the protection's economic impact,

we ask: *Does higher legal protection for security researchers imply a lower bounty and an increased cost of a BBP?* We find that, interestingly, an organization may need to provide a higher bounty or may obtain more benefit in a BBP if the level of legal protection is higher, depending on the nature of the different cost structures.

3.1.3 Literature Review

Economics of cybersecurity.

As cyber threats continuously escalate, an increasing number of organizations prioritize cybersecurity spending (Business Wire 2020). Therefore, the cost-effectiveness of specific cybersecurity solutions becomes vital (Blizard 2020). In particular, it is critical for many organizations with limited resources and IT security capability to strike a balance between “perfect security” and “economic viability.” Literature on the economics of cybersecurity extensively investigates the optimal resource allocations and mechanism design (e.g., Hui et al. 2019, August et al. 2019, Kannan et al. 2016) in improving the security outcomes of organizations in various contexts such as investments in general IT security protection (Chen et al. 2011, Gordon and Loeb 2002), contracting with managed security service providers (Hui et al. 2019, Cezar et al. 2014, Lee et al. 2013), or sharing cybersecurity information (Gal-Or and Chose 2005).

Our study complements this stream of literature by focusing on a specific context of substantial information security implications, i.e., the economics of vulnerability management. First, we examine a BBP as a “proactive defense strategy.” In other words, organizations need to prepare for incoming vulnerability reports. Unlike literature that mostly considers the cases where organizations receive unsolicited vulnerability reports (Kannan and Telang 2005, Arora et al. 2008), we investigate the optimal design of a cybersecurity crowdsourcing program where organizations carefully assess main metrics before starting their BBPs. Therefore, we formally analyze several factors that an organization needs to carefully consider in improving the cost-effectiveness of its program, which has seldom been discussed in the literature.

Second, our model captures the main characteristics of crowdsourcing in the vulnerability discovery process (e.g., the group size of security researchers and heterogeneity of their efficiency levels), which is a departure from literature where only one security researcher can facilitate vulnerability discovery (Arora et al. 2008, Cavusoglu et al. 2008). Therefore, our work can offer several new managerial insights for organizations and policymakers.

Bug bounty programs.

As more organizations adopt BBPs and the community of security researchers grows, an increasing number of studies collect both quantitative and qualitative data, providing different perspectives on whether or not BBPs are cost-effective (Sridhar and Ng 2021, Walshe and Simpson 2020, Hata et al. 2017). Many argue that BBP is economically efficient for two main reasons. First, a large group of researchers can expedite the discovery of vulnerabilities (Schechter 2002). Second, organizations can reward only those who first discover the vulnerability (Malladi and Subramanian 2019). However, these discussions are inconclusive because of a lack of examination of vulnerability's lifecycle, which is key to the organization's payoffs in managing the BBPs.

The setting that we examine is similar to that of Zhao et al. (2017) who sheds light on misaligned incentives between security researchers and organizations, and then evaluates the effectiveness of different policies. However, our study differentiates from this paper and other BBP studies in considering the BBP as a layer in the vulnerability management process. While other studies look at the payoffs of a BBP based on the probability of discovering the vulnerability, we focus on the lifecycle of a vulnerability which enables our model to yield more realistic findings and practical insights into managing BBPs.

Innovation crowdsourcing.

BBP is a type of crowdsourcing program because “there is a defined crowd with a clear goal and a defined benefit for both the worker and requester” (Fryer and Simperl 2017, p.3). Furthermore, rather than labor tasks where the workloads are specific, vulnerability discovery in BBPs is a process of generating innovative outputs (Ransbotham and Ramsey 2012). Therefore, the literature on innovation crowdsourcing is more related to our work. This literature stream focuses on the behavior of a crowd of participants and investigates the optimal incentive schemes (e.g., Hu and Wang 2021, Mo et al. 2019, Zhang et al. 2019, Huang et al. 2014, DiPalantino and Vojnovic 2009, Terwiesch and Xu 2008).

BBPs have two main crowd-based characteristics: *time-based* and the *winner-takes-all*. First, the main purpose of a BBP is to identify vulnerabilities earlier since the earliest discovery time is critical for organizations to become aware of the vulnerability and take measures to reduce potential risks (Arora et al. 2008, Kannan and Telang 2005). Second, the winner-takes-all naturally implies that only one winner can be awarded the prize (or bounty) in the tournament, as this approach is regarded as the optimal strategy in several settings (Terwiesch and Xu 2008, Moldovanu and Sela 2001). In practice, as most BBPs adopt the winner-takes-all approach, we capture these crowdsourcing characteristics in our models.

Unlike this stream of literature, our study further captures more security characteristics of BBPs, including collaboration and conflicts between the organization and security researchers. First, we examine the characteristics of security researchers and the organization in the same model due to the collaboration pattern in BBP in identifying and remediating the vulnerability. Therefore, taking these dynamics into consideration can provide new practical implications for organizations in BBPs.

Second, we consider the main risks in BBP - there might be a leak out of the participants in the BBP. Thus, an organization might face some post-discovery costs. By capturing these effects, our study fills important gaps in the literature.

3.2 Model

In practice, a BBP involves a group of security researchers and an organization that we capture in our model. We consider a static game with incomplete information since the productivity of each security researcher can not be observed. Next, we discuss how we characterize them in detail. Table 3.1 summarizes the key parameters and variables.

Table 3.1. List of Key Parameters and Variables

Parameters	Definitions
a_i	Productivity of security researcher i , where $\underline{a} \leq a_i \leq \bar{a}$
c	Effort cost coefficient of security researchers
l	Legal protection, where $0 \leq l \leq 1$
c_a	Damage cost coefficient
c_p	Post-discovery cost coefficient
β	Level of security posture, where $0 \leq \beta \leq 1$ (0 is the strongest and 1 is the weakest)
ω	Patching complexity
θ	PR effect coefficient
T	Vulnerability complexity
Variables	Definitions
e_i	Effort level of security researchers i
b	Bounty cost
I	Earliest discovery time
D	Damage Cost
K	Post-discovery cost
Π	Total cost of a bug bounty program

3.2.1 Security Researchers

Security researchers are independent individuals who work to discover a security vulnerability for the benefit of the organization. In practice, to incentivize the security researchers to exert a higher level of effort in discovering vulnerabilities and thereby lower potential security risks, an organization announces a bounty as a reward in its BBP (Laszka et al. 2018).

The major advantage of a BBP lies in the power of the crowd as a whole but not one specific individual participating in the program. However, a BBP’s overall performance needs to be inferred from the characteristics of individual security researchers. Therefore, we next discuss individual security researchers and how their characteristics affect the vulnerability discovery process. In a BBP, each security researcher determines her effort level depending on her expected payoff. Similar to other crowdsourcing or tournament settings, a higher reward can elicit higher levels of effort from security researchers (Laszka et al. 2018). Furthermore, BBPs are similar to winner-take-all contests as only the first security researcher that reports the vulnerability is rewarded the bounty (Bugcrowd 2015). Therefore, the expected payoff is contingent on the probability that the security researcher is the first to submit the valid vulnerability report. Furthermore, the payoff also depends on the likelihood that a security researcher will not be facing a backlash from the organization and indeed receive the bounty (Gamero-Garrido et al. 2017). Next, we explain the details.

Tournament among security researchers.

A BBP is similar to a winner-take-all tournament. Specifically, only the participant who has the best performance can win the bounty. The main purpose of a BBP is to reduce the earliest discovery of a vulnerability. To characterize our setting, we utilize a productivity-based project model (e.g., see Körpeoğlu and Cho 2018).² Hence, the discovery time of each security researcher can be regarded as their “per-

²Other types of models such as cost-based and expertise-based models can be converted to and represented as productivity-based projects (Körpeoğlu and Cho 2018).

formance” that is the focus of tournament literature (e.g., Archak and Sundararajan 2009, Terwiesch and Xu 2008)

In the “tournament,” each security researcher i is endowed with productivity or efficiency (i.e., a_i) in discovering a security flaw (Shrobe et al. 2018). This productivity is related to the level of security knowledge and skills. Each security researcher i makes effort e_i , at unit cost c , to improve their performance in searching for vulnerabilities. For example, security researchers usually spend time on conducting (basic) forensic analysis, trying different attacking methods, or figuring out potential remediation (Zhao et al. 2017).

Therefore, security researcher i ’s performance is jointly determined by her productivity a_i and effort e_i . We characterize the performance g_i as a product of individual productivity and effort (i.e., $a_i e_i$) similar to the related literature (e.g., see Körpeoğlu and Cho 2018). Because the “discovery time” decreases in performance (i.e., the vulnerability is discovered earlier), we characterize it as $T - a_i e_i$, where T is the time point that the vulnerability is nullified (i.e., the service or product is upgraded or terminated).

A security researcher’s winning probability depends on her and others’ performances. Similar to tournament settings, we consider that the number of security researchers (i.e., n) and the distribution of productivity Q (i.e., $Q \sim U[\underline{a}, \bar{a}]$) is common knowledge to all (e.g., see Terwiesch and Xu 2008, Stouras et al. 2021). Since security researcher i ’s performance is g_i , winning the bounty requires that her performance is better than others, which is $P(g_i > g_j) \forall j \neq i$. Hence, the probability of identifying the vulnerability faster than the other security researchers can be written as $P(g_i > g_{-i}) = Q_{(1)}^{n-1}((Q_{-i})^{-1}(g_i))$, where $Q_{(1)}^{n-1}(g_i)$ denotes the probability of winning the bounty. However, unlike the tournament literature, the winning of the reward (or the bounty in our case) does not solely depend on being the best security researcher. In particular, winning the bounty also depends on the legal framework that the BBP is based on. We discuss the details next.

Perceived benefits of participating in a BBP.

A BBP has high levels of uncertainty for security researchers as even being the fastest security researcher does not necessarily mean that she will receive the reward. This is in fact one of the most debated topics in the BBP context (Gamero-Garrido et al. 2017). In particular, there are legal risks in participating in BBPs. Security researchers may be disincentivized in searching for a vulnerability because of legal issues. Although some BBPs have certain policies aiming to mitigate this issue, the legal scope is ambiguous (Elazari 2018). For instance, some programs state that “You may not attempt to gain unauthorized access to any solution or to networks connected to it, or to content stored or delivered through it,, including by hacking, spoofing or seeking” The definition of “authorization” and “hacking” is rather unclear (J.M.Porup 2018). Some BBPs adopt “safe harbor clauses,” promising not to pursue legal action against security researchers. Therefore, security researchers may face different levels of legal protection while participating in different BBPs.

To capture this impact, we denote the legal protection toward security researchers is l , where $0 \leq l \leq 1$. The legal protection term l also impacts the firm in a nuanced way. At one extreme, if there is no legal protection (i.e., $l = 0$), we consider that the security researchers do not participate in the BBP as they consider it a “witch hunt.” On the other extreme, if there is complete protection (i.e., $l = 1$), then the security researchers may be relaxed, and the leaks out of the program may be a greater concern to the firm. Therefore, the parameter l , which depends on the environmental factors (such as laws and industrial standards) also impacts the costs of the firm that we discuss in detail in Section 3.2.2.

In summary, a group of security researchers search for the vulnerability. They set their effort levels depending on perceived benefits, productivity, effort costs, and other participants’ efforts. However, they may be disincentivized in searching for a vulnerability because of legal issues. The legal protection term l , in effect, adjusts the security researchers’ beliefs that they will indeed receive the bounty even if they are the first to discover the vulnerability. Therefore, by utilizing the arguments in

Sections 3.2.1 and 3.2.1, we can write the expected net payoff of security researcher i as: $\pi_i = blQ_{(1)}^{n-1}((g_{-i})^{-1}(g_i)) - ce_i$. Next, we discuss the characteristics of organizations in our setting.

3.2.2 Characteristics of the Organization

Vulnerability management is essential in controlling information security risks in organizations (Barillon 2019). It mainly involves vulnerability identification and vulnerability remediation (Cavalancia 2020). BBP, as a crowdsourced security solution, can leverage external help and facilitate vulnerability identification. The organization needs to decide on the amount of *bounty* or the reward if it holds a BBP as a layer in its vulnerability management process. Along with the cost of the bounty, the organization encounters two other types of costs: *expected damage cost* and *expected post-discovery cost*. Then, the organization that employs a BBP has an incentive to manage the BBP such that the total cost related to the vulnerability threat (i.e., damage cost) and cost related to BBP (i.e., post-discovery cost) is minimized. Next, we explain each of these cost components in detail.

Bounty cost.

In a BBP, a *bounty* is a reward (generally of monetary nature) provided for the discovery of a vulnerability to a group of security researchers (Malladi and Subramanian 2019). We denote the bounty by b , which is a decision variable for the organization. As discussed earlier, setting a proper bounty is an important strategy to elicit efforts from security researchers. For example, if the amount is too low, security researchers would exert lower levels of effort, leading to a delay in the identification of the vulnerability. Also, as explained in Section 3.2.1, although the first security researcher that identifies the vulnerability might not be awarded the bounty because of the legal framework that the bounty is based on, we consider that there will at least be one security researcher who identifies the vulnerability and acts within the legal scope of the BBP. Hence, we focus on the BBPs where the bounty is awarded to a secu-

rity researcher and do not provide the solutions for other scenarios that are not very interesting.

Expected damage cost.

Vulnerabilities can be leveraged to get illegal access to organizations' networks and systems, causing substantial damage. From the perspective of vulnerability management and organizational security management, several key factors impact the magnitude of these damages that we explain next.

Organization's security posture. If a vulnerability is being exploited, the damage cost it incurs will be substantially affected by the level of its security posture, which is defined as "the security status of an enterprise's network, information, and system based on information security resources (e.g., people, hardware, software, policies) and capabilities in place to manage the defense of the enterprise and to react as the situation changes." (Dempsey et al. 2012, page B-13) To assess security posture, the National Institute of Standards and Technology (NIST) introduced several cybersecurity frameworks that provide various security metrics in key areas such as risk management processes, security technologies, and implementation (e.g., NIST 2014). Based on the cybersecurity framework, a variety of related standards and models (e.g., IOS, ITIL, SANS, Forrester Research³) are established. These standards and models share similar characteristics and enable organizations to evaluate their security posture that we denote with β , where we consider that $0 \leq \beta \leq 1$. The lower the β is, the stronger an organization's security posture is.

As a proxy of an organization's overall security capability, security posture can substantially impact the efficacy of vulnerability management in two main aspects. First, a strong security posture is negatively associated with the rate of damage caused by the exploitation of the vulnerability. The main reason is that a strong security posture indicates that an organization has a smaller attack surface (also known as the attack vector), which means that effective measures are adopted to provide a higher

³<https://www.forrester.com/report/Gauge-Your-Information-Security-Maturity/RES157656>

level of protection (Robinson 2017). For instance, effective network segmentation can prevent attackers' lateral movement, thereby lowering the damage loss (Andress and Leary 2016). We consider that the base level of the damage cost \hat{c}_a is i.i.d. and follows a general distribution Λ_a . We denote the mean (i.e., $\int_{\Lambda_a} \hat{c}_a dx$) of this parameter with c_a and use it in the analysis hereafter as the unit damage cost. Therefore, if we denote the base level of the damage cost with c_a , we can present the damage cost as $\beta \hat{c}_a$ since β (i.e., security posture) represents the extent of realized damage cost. This damage cost accrues through the life cycle of the vulnerability that will be discussed later.

Second, an adequate level of security posture enhances the patching capability (Robinson 2017). For many organizations, patching is costly and is believed to impact productivity negatively. Specifically, it may necessitate planned downtime for maintenance, and some unexpected errors may disrupt operations during patching (Cavusoglu et al. 2008). However, the frictions in patching can be substantially lower if an organization has clear maintenance plans and can implement these plans effectively. Based on these facts, we denote ω as the patching complexity coefficient and $\omega\beta$ as the realized patching time. This formulation suggests that an increased security posture is negatively associated with the realized patching time.

In many settings, increasing the IT security capability to tackle a vulnerability in a short-term horizon is not possible, because hiring IT security staff that can understand the inner workings of the software application or infrastructure is generally a long-term endeavor (Petersen 2019). Therefore, in our main model, we consider that the time needed to fix a vulnerability is constant (i.e., $\omega\beta$ is exogenous). However, in the extension model we consider in Section 3.5.2, we endogenize the parameter β . The results of this extension model are qualitatively similar to our main model.

Lifecycle of the vulnerability. Life-cycle of the vulnerability consists of two main phases: a pre-discovery phase and a post-discovery phase. The pre-discovery phase refers to the duration from announcing the bounty to receiving the first vulnerability report (i.e., 0 to $\mathbb{E}[I]$). The post-discovery phase refers to the duration from the earliest discovery time to the time when the organization fixes the vulnerability

(i.e., $\mathbb{E}[I]$ to $\mathbb{E}[I] + t_p\beta$). Therefore, $\mathbb{E}[I] + t_p\beta$ can also be regarded as the length of the life-cycle of the vulnerability.

One key performance metric of a BBP is the expected earliest discovery time, i.e., $\mathbb{E}[I]$. This process can be considered as a technological innovation that is generally of high uncertainty in the literature rather than purely deterministic (Mitra and Ransbotham 2015). In BBPs, the expected earliest discovery is determined based on the individual security researchers' performance vector v , the number of security researchers n , and the distribution of productivity $H \sim U[\underline{a}, \bar{a}]$. In particular, we can compute the best performance as $\int_{\underline{a}}^{\bar{a}} g_i h_{(1)}^n(a) da$, where $H_{(1)}^n(a)$ is the first order statistic and $h_{(1)}^n(a)$ is the derivative of $H_{(1)}^n(a)$.

Public relations (PR) effect. When the security of the network or system of an organization is compromised, the organization often suffers significant financial losses due to lost sales, customer goodwill, reputation, or digital assets (August et al. 2014). Interestingly, in practice, a BBP can help offset the financial losses partially - regardless of the success of the BBP per se in discovering the vulnerabilities (Kaczanowski 2020). This is mainly because an organization usually announces BBP to the public, and there is mass media coverage.

Many businesses are engaged in BBPs or increase their commitments to BBPs when they experience security crises. For example, in April 2020, after receiving public scrutiny and criticism about security, Zoom revealed that it enhanced its BBP and aimed to mitigate public concerns.⁴ Similarly, Hyatt launched its BBP after the mega data breach of its industry peers Marriott.⁵ Furthermore, since a higher bounty is perceived by the public a bigger commitment to security, we normalize the damage cost accrued by the firm through the lifecycle of the vulnerability by $1 - \theta b$. Here, θ is the coefficient that denotes the efficiency of the public relations (PR) effect, which implies that the reduction in the damage cost (as a percentage) is θb , and $0 \leq \theta b \leq 1$. If there is no PR effect in a given BBP, then θ can be set to zero to represent this scenario.

⁴<https://www.tomsguide.com/news/zoom-security-privacy-woes>

⁵<https://www.infosecurity-magazine.com/news/hyatt-first-major-hotel-chain-to/>

Base damage cost. To summarize, to compute the base damage cost, the unit damage multiplier (i.e., c_a) should be adjusted based on the organization’s security posture (i.e., β). This cost accrues during the life-cycle of the vulnerability (from 0 to $\mathbb{E}[I] + \omega\beta$), and the magnitude might be reduced because of the PR effect (i.e., θb). Therefore, base damage cost can be written as $\int_0^{\mathbb{E}[I] + \omega\beta} c_a \beta (1 - \theta b) dt$.

Expected post-discovery cost.

Although the damage cost discussed in the previous section “also” applies during the post-discovery phase (i.e., from $\mathbb{E}[I]$ to $\mathbb{E}[I] + \omega\beta$), there is an additional concern in practice that there might be a leak from the set of security researchers participating in the BBP (Crews et al. 2018). This leak might not need to be as comprehensive as a submitted vulnerability report, but still might put the operations of the organization in jeopardy (Arora et al. 2008). We consider that the base level of the post-discovery cost \hat{c}_p is i.i.d. and follows a general distribution Λ_p . We denote the mean (i.e., $\int_{\Lambda_p} \hat{c}_p dx$) of this parameter with c_p and utilize it in our analysis hereafter as the unit post-discovery cost. The total post-discovery cost would be positively associated with the level of participation in the BBP that we represent with bn as a proxy. Furthermore, as discussed earlier, the legal protection offered to the participants (by law) in the BBP is, in fact, one of the most debated topics in the BBP context (Gamero-Garrido et al. 2017). As a higher level of legal protection gives an opportunity to security researchers to be more relaxed in their search process, and also entices them to exert more effort in the bounty (i.e., the effect of l on the effort levels e^*), the level of legal protection also increases the total post-discovery cost.

Therefore, we normalize the post-discovery cost by l . Last, the exposure to this possible leak is from when the vulnerability is discovered first to until it is mediated (i.e., from $\mathbb{E}[I]$ to $\mathbb{E}[I] + \omega\beta$ as shown in Section 3.2.2). Hence, we compute the post-discovery cost as $\mathbb{E}[K] = \int_{\Lambda_p} \int_{\mathbb{E}[I]}^{\mathbb{E}[I] + \omega\beta} \hat{c}_p bnl dt dx = \int_{\mathbb{E}[I]}^{\mathbb{E}[I] + \omega\beta} c_p bnl dt$.

Considering all the cost components, the organization wants to minimize the expected total cost in the BBP by deciding the amount of bounty. The question can then be written as:

$$\min_b \mathbb{E}[\Pi] = b + \int_0^{\mathbb{E}[I] + \omega\beta} c_a \beta (1 - \theta b) dt + \int_{\mathbb{E}[I]}^{\mathbb{E}[I] + \omega\beta} c_p b n l dt \quad (3.1)$$

3.2.3 Sequence of the Game

We capture all the dynamism discussed so far in a two-stage game. In the first stage, an organization announces a bounty to the public for uncovering the vulnerability in their IT infrastructure or digital products. In the second stage, observing the bounty, a group of security researchers exerts effort to identify the security flaw. In particular, the second stage consists of two main phases: the pre-discovery phase and the post-discovery phase. The pre-discovery phase starts from time 0 and ends with $\mathbb{E}[I]$, which is the time when the vulnerability is firstly reported by a security researcher. Next, the organization starts to patch the reported vulnerability at $\mathbb{E}[I]$, and it takes $\omega\beta$ (i.e., patching time) to fix the vulnerability. Therefore, the patching time determines the length of the post-discovery phase. The end of this phase implies that the vulnerability is fixed and causes no threat. We use backward induction to derive solutions and present them in the next section.

3.3 Solutions

We first obtain the optimal decisions of each security researcher given a bounty b by using backward induction. Observing the bounty announced by the organization (i.e., b), security researchers exert different effort levels to find the vulnerability in the second stage of the game. We compute the individual-level utility maximizing effort levels of each security researcher as follows. All primary proofs are available in the Appendix.

We first use backward induction to solve the optimal effort of security researchers.

Lemma 3.3.1 *Given the bounty b , and legal protection l , each security researcher i exerts effort:*

$$e_i^* = \frac{bl \left(\frac{a_i - \underline{a}}{\bar{a} - \underline{a}} \right)^{n-1} (\underline{a} + (n-1)a_i)}{cna_i}.$$

The results reveal several findings. Intuitively, the magnitude of bounty and legal protection is positively associated with security researchers' effort levels and the expected earliest discovery time, while the cost of effort exerts an opposite effect. Furthermore, the decision and performance of security researchers are non-monotonic in the number of security researchers. On the one hand, a higher number of security researchers may elicit a higher level of competition which lowers the probability of winning, providing a disincentive to security researchers. On the other hand, a higher bounty increases the expected performance of the runner-up (i.e., competing security researchers), thereby encouraging security researchers to exert a higher level of effort. These findings are in line with the literature on crowdsourcing and tournaments (e.g., see Körpeoğlu and Cho 2018).

By taking into account the equilibrium effort levels presented in Lemma 3.3.1, the organization computes the optimal bounty as presented in Lemma 3.3.2.

Lemma 3.3.2 *At the equilibrium, the organization sets the bounty as:*

$$b^* = \frac{1}{2\theta} - \frac{2cn(2n-1)(-\beta\theta c_a(\beta\omega + T) + \beta \ln \omega c_p + 1)}{2\theta\beta l c_a((n-1)(2n-1)\bar{a} + (3n-1)\underline{a})}.$$

For brevity, we do not provide a discussion of how the optimal bounty changes with respect to model parameters as most of these results are intuitive. One of the key success measures for BBPs is having an early detection time of the vulnerability because the discovery of the vulnerability is the antecedent of remediation in the vulnerability management pipeline (Alomar et al. 2020). Furthermore, another important measure in the BBP is the total post-discovery cost. Therefore, we next present these measures in Corollary 3.3.1. These expressions are further utilized in deriving some other results and managerial insights.

Corollary 3.3.1 *(i) The equilibrium expected earliest discovery time of the vulner-*

$$ability is: \frac{1}{4} \left(2T + \frac{l(((3-2n)n-1)\bar{a}-3n\underline{a}+\underline{a})}{c\theta n(2n-1)} + \frac{2\beta\omega(\ln c_p - \beta\theta c_a) + 2}{\beta p r c_a} \right)$$

(ii) The equilibrium total post-discovery cost is: $\frac{n\omega c_p}{2\theta} \left(\beta l - \frac{2cn(2n-1)(-\beta\theta c_a(\beta\omega+T)+\beta l n\omega c_p+1)}{c_a((n-1)(2n-1)\bar{a}+(3n-1)\underline{a})} \right)$.

These results have several managerial insights and implications that we discuss detail in the next section.

3.4 Results and Managerial Insights

We present our results based on how the performance and dynamics of the BBP are impacted by the characteristics of (i) the organization, (ii) security researchers, and (iii) the legal underpinnings of the BBP.

3.4.1 How Do the Organization's Characteristics Impact the Bounty?

In this section, we focus on how the BBP related characteristics of the organization, such as (i) patching complexity and (ii) the security posture of the organization, impact the dynamics and the performance of the bounty. An increasing number of organizations in different industries, including big tech firms (e.g., Microsoft, Google), traditional businesses (e.g., Healthcare, Retail), and government agencies (e.g., Department of Defense, Air Force), establish their BBPs. While the purpose of having the BBP is the same, the organization's characteristics can significantly determine the dynamics of a BBP mainly because of two factors: the security posture of the firm (i.e., β) and patching complexity (i.e., ω).

As discussed in the motivation section, vulnerability management consists of two main stages: vulnerability discovery and vulnerability remediation (Ransbotham and Ramsey 2012, August and Tunca 2006, Kannan and Telang 2005). The organization is responsible for the vulnerability remediation stage, and the security posture of the firm (i.e., β) impacts both the patching time and the damage cost perceived by the organization through the life cycle of the vulnerability. Second, the organization's size and type of its digital asset influence the patching frictions or complexity of the vulnerability (i.e., ω) as vulnerabilities in sophisticated and distributed IT systems are argued to be more complex than other vulnerabilities (Souppaya and Scarfone

2022). For instance, vulnerabilities in core IT systems may create a longer downtime or cause more operational problems (Shein 2022). Although practitioners advocate that organizations need to assess their security features when incorporating BBP as a layer in vulnerability management (e.g., see Cassin 2020 and Marino 2020), there are no formal analyses on how to design a bounty based on these characteristics. Therefore, we ask: *Does a higher patching complexity or a weaker security posture imply a lower bounty?* Proposition 3.4.1 addresses this question.

Proposition 3.4.1 (i) *If the patching complexity of a vulnerability (i.e., ω) is higher, the organization may have a higher bounty if the security posture of the organization is sufficiently weak (i.e., β is high). In other words, $\frac{\partial b}{\partial \omega} > 0$ iff $\beta > \frac{Inc_p}{\theta c_a}$.*

(ii) *If the security posture of the organization is stronger (i.e., β is lower), the optimal bounty is lower. In other words, $\frac{\partial b}{\partial \beta} > 0$.*

As discussed before, vulnerability management consists of two main stages: vulnerability discovery and vulnerability remediation. Because a higher patching complexity implies a slower response in remediating the vulnerability and an increased post-discovery cost, one may consider that the organization may lower the bounty to reduce the post-discovery cost. However, part (i) of Proposition 3.4.1 implies that such a substitutive nature of the bounty and remediation is not necessarily correct. The proof reveals that the marginal effect of the bounty in lowering the damage cost increases in patching complexity (i.e., $\frac{\partial^2 D}{\partial b \partial \omega} < 0$). Furthermore, the patching complexity is positively associated with the marginal effect of a bounty in increasing the cost incurred in the post-discovery stage (i.e., $\frac{\partial^2 K}{\partial b \partial \omega} > 0$). Hence, the magnitude of these changes in the marginal effects of a bounty determines how an organization needs to adjust the bounty. In particular, we find that if the security posture of the firm is weak (i.e., β is high), the effect on the damage cost dominates the effect on the post-discovery cost, i.e., $|\frac{\partial^2 D}{\partial b \partial \omega}| > |\frac{\partial^2 K}{\partial b \partial \omega}|$ if $\beta > \frac{Inc_p}{\theta c_a}$. Therefore, the organization is incentivized to increase its bounty even if the patching complexity is higher. On the

other hand, if the security posture is strong (i.e., $\beta < \frac{inc_p}{\theta c_a}$), the organization considers the bounty as substitutive to its remediation if the patching complexity is higher.

Part (ii) of the proposition next reveals that the organization prefers a lower the bounty if its security posture is better (i.e., β is lower). We omit the theoretical explanation of this result for brevity, but it depends on the reduction in both damage and post-discovery costs.

The results provide insights on how to design a bounty based on two key security features of the organization: patching complexity and security posture. While setting up a BBP, the organization needs to incorporate its own security characteristics. Specifically, an organization's patching frictions/complexity is contingent on the size and type of its digital asset. For instance, patching complexities for organizations that rely more on remote workings is higher because of the challenges in managing distributed workforces and endpoints (Comeau 2021). This is especially important in a BBP since a long patching time introduces additional risks and costs to the organization. For instance, United Airlines's delays in patching trigger the backfire of its BBP (Storm 2015). Furthermore, the security posture of the organization can directly affect the efficacy of a high bounty. In contrast to the arguments that organizations that have a stronger security posture need to offer a higher bounty to provide more incentive to the security researchers, our results shed light on the substitutive role of organizations' own security posture and a bounty. To improve the cost-effectiveness of a BBP, organizations with a lower security posture should offer a higher bounty to elicit earlier discovery of a vulnerability.

Proposition 3.4.1 contributes to the literature in several ways. First, to the best of our knowledge, it is the first formal attempt to examine how security characteristics of an organization affect the optimal bounty in a BBP. Although discussed in practice (e.g., Marino 2020), there are no studies that consider the interplay between post-discovery costs and the setting of the bounty. We investigate the role of this important and unique feature in BBPs and contribute to the literature.

3.4.2 How Do Security Researchers Impact the Bounty and the Total Cost of the BBP?

In this section, we first examine how the characteristics of security researchers, including the heterogeneity in their productivity and the total number of them, affect the optimal bounty and the total cost of the BBP.

Optimal bounty.

In the broader context of crowdsourcing, a group of participants can contribute significantly to projects by generating innovative outputs (Boudreau et al. 2011). Similarly, in a BBP, a group of security researchers also work on the same IT infrastructure or digital products, facilitating the discovery of vulnerabilities. Specifically, two dimensions of the security researchers group are keys to a BBP: their (i) productivity and (ii) total number. Although the crowdsourcing literature investigates how to design the optimal bounty considering participants' characteristics and task structure, the results are mixed in various settings (Boudreau et al. 2011, Terwiesch and Xu 2008). Because we consider that a BBP is different from typical crowdsourcing tasks in terms of the collaboration pattern and potential risks, there is no guidance in the literature regarding this issue, although this issue is debated in practice (Haynes and Sadeghipour 2021, Bracken 2021). Therefore, it is important to examine the role of characteristics of security researchers in a BBP and how they affect an organization's decisions in the BBP. Therefore, more specifically, we ask: *Does having more productive security researchers or having a larger number of security researchers in the BBP correspond to a lower bounty?* We address this question in Proposition 3.4.2.

Proposition 3.4.2 (i) *If security researchers' productivities (i.e., \underline{a} or \bar{a}) are higher, the organization may need to have a higher bounty. This happens if and only if the efficiency of PR effect is small (i.e., $\theta < \frac{\beta \ln \omega c_p + 1}{\beta c_a (\beta \omega + T)}$).*

(ii) *If the number of security researchers (i.e., n) is higher, the organization may need to have a higher bounty. This happens if and only if:*

- (a) the heterogeneity of security researchers' productivity is small (i.e., $\frac{\bar{a}}{a} \leq \frac{6n^2-4n+1}{(1-2n)^2}$) but the efficiency of PR effect is large (i.e., $\theta > \hat{\theta}_1(\frac{\bar{a}}{a}, \cdot)$), or
- (b) the heterogeneity of security researchers' productivity is large (i.e., $\frac{\bar{a}}{a} > \frac{6n^2-4n+1}{(1-2n)^2}$) but the efficiency of PR effect is small (i.e., $\theta < \hat{\theta}_1(\frac{\bar{a}}{a}, \cdot)$). $\hat{\theta}_1 = \frac{a(12\beta \ln^3 \omega c_p + n^2(6-9\beta \ln \omega c_p) + 2n(\beta \ln \omega c_p - 2) + 1) + (1-2n)^2 \bar{a}(\beta \ln(n-2)n \omega c_p - 1)}{\beta c_a((-6n^2+4n-1)\bar{a} + (1-2n)^2 \bar{a})(-\beta \omega - T)}$.

We first discuss part (i) of Proposition 3.4.2. One may think that if the security researchers are more efficient, the organization can have a lower bounty to improve BBP's cost-effectiveness. However, the proposition suggests that the organization may need to have a higher bounty. It happens if the efficiency of the PR effect (i.e., θ) is small. Ceteris paribus, having higher efficiency levels leads to an increase in the marginal effect of the bounty in shortening the earliest discovery time by incentivizing security researchers ($\frac{\partial^2 \mathbb{E}[I]}{\partial b \partial a} < 0$). Nevertheless, it reduces the magnitude of the PR effect in lowering the damage cost ($\frac{\partial^2 (1-b\theta) \mathbb{E}[I]}{\partial b \partial a} > 0$). It is mainly because these two effects are substitutes for reducing the damage cost. Therefore, whether increasing or decreasing the bounty depends on the magnitude of the PR effect (i.e., θ). In particular, if the PR effect is substantially small (i.e., $\theta < \frac{\beta \ln \omega c_p + 1}{\beta c_a (\beta \omega + T)}$), then increasing the bounty is more beneficial to the organization.

Next, we discuss part (ii) of Proposition 3.4.2. The number of participants is regarded as a critical measure of a crowdsourcing program. One might think that an organization can lower the bounty if there are more contributions from a larger crowd. Nevertheless, our results show that it is not always optimal. Interestingly, there are two cases under which the organization may need to have even a higher bounty as we explain next.

First, security researchers change their strategies because a larger crowd affects the probability of winning the bounty. In a "winner-take-all" setting where only the best (or the quickest as in our setting) solution wins the award, the number of participants has subtle effects on security researchers' effort levels. Specifically, two competing effects are at play, which is consistent with the tournament literature (e.g., see Körpeoğlu and Cho 2018). The first is the *competition effect*, suggesting that an

individual participant in a tournament perceives a lower probability of winning the bounty if the number of participants increases, thereby reducing their incentives to exert effort. The second effect is the *runner-up effect*, indicating that a larger group size increases the expected performance of the runner-up and thereby creates an incentive to exert more effort for the winner (and possibly some other participants). Therefore, increasing the number of security researchers induces asymmetric impacts on security researchers with different levels of productivity. On the other hand, the PR effect impacts the organization's decisions, although it does not directly influence the security researchers.

The proof of part (ii) of Proposition 3.4.2 reveals that if a larger crowd of security researchers participates in the BBP, the organization needs to have a higher bounty in two cases. First, the heterogeneity across the security researchers in terms of their productivity is small (i.e., $\frac{\bar{a}}{a} \leq \frac{6n^2-4n+1}{(1-2n)^2}$) and the magnitude of the PR effect is large (i.e., $\theta > \hat{\theta}_1$), or second, the heterogeneity is high but the PR effect is small. First, if the heterogeneity across the security researchers in terms of their productivity is small (i.e., $\frac{\bar{a}}{a} \leq \frac{6n^2-4n+1}{(1-2n)^2}$) and the number of security researchers increases, security researchers' best performance is lower (i.e., the earliest discovery time of the vulnerability takes longer) as the competition effect dominates. Therefore, the marginal effect of the bounty in reducing the expected earliest discovery time is lower (i.e., $\frac{\partial^2 \mathbb{E}[I]}{\partial b \partial n} > 0$).

However, the marginal effect of the bounty in mediating the PR effect increases because the vulnerability is expected to be discovered later if the bounty is decreased (i.e., $\frac{\partial^2 (1-b\theta) \mathbb{E}[I] c_a}{\partial b \partial \theta} < 0$). Furthermore, a larger crowd also increases the marginal effect of the bounty in increasing the post-discovery cost (i.e., $\frac{\partial^2 K}{\partial b \partial n} > 0$). Therefore, if the efficiency of the PR effect in offsetting the damage cost is sufficiently high (i.e., $\theta > \hat{\theta}_1$), the marginal effect of a bounty in reducing the damage cost outweighs the marginal effect of the bounty in increasing the post-discovery costs. As a result, the organization prefers to have a higher bounty if the heterogeneity of the security researchers is small and the PR effect is high. Hence part (ii)(a) of the proposition. Second, let us discuss when part (ii)(b) of Proposition 3.4.2 holds. Because the

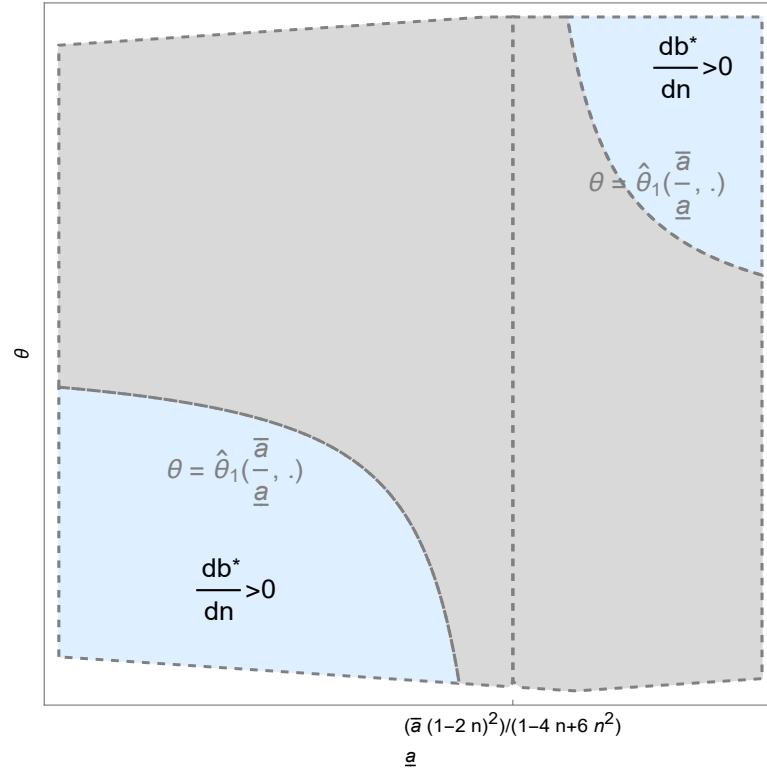


Figure 3.1. The Marginal Effect of an Additional Security Researcher on the Optimal Bounty as a Function of Productivity Heterogeneity $\frac{\bar{a}}{a}$ and PR Effect θ

efficiency of the PR effect is now small (i.e., small θ), the explanation now depends on the competition and the runner-up effects of the increase in the number of security researchers. In particular, if the heterogeneity among the security researchers is sufficiently high (i.e., $\frac{\bar{a}}{a} > \frac{6n^2-4n+1}{(1-2n)^2}$), the proof reveals that the runner-up effect dominates the competition effect. Hence, the organization prefers to have a higher bounty again. Figure 3.1 highlight the blue regions where the number of security researchers implies a higher amount of bounty.

Proposition 3.4.2 helps us glean the following practical insights regarding how two key dimensions of security researchers - the productivity and the total number, affect the optimal bounty. The security researchers' productivities may be higher if there is better access to technological innovation (e.g., automated penetration testing tools), or the number of security researchers in a BBP may be higher if the organization

becomes more popular. Unlike the discussions in practice that argue that (i) having a more talented (or more efficient) group of security researchers, or (ii) a larger crowd in the BBP can help an organization have a lower bounty, we find that these dynamics are rather nuanced. In fact, how the bounty should be adjusted based on the heterogeneity across the security researchers and the PR effect is another topic of debate in the BBP domain per se (e.g., see Hata et al. 2017, Terrill 2018). Therefore, managers should pay more attention (i) to the efficiency of the PR effect, although it is not a security researcher-driven dynamic, and (ii) to heterogeneity rather than simply to the magnitude of productivity and the crowd size. This result is also observed in practice. For example, Zoom is cited as increasing its BBP after significant public scrutiny (and hence the number of security researchers in its BBP) because of the PR effect (Osborne 2022, Cimpanu 2020).

From a theoretical viewpoint, we consider security researchers' characteristics in a BBP, which is a missing piece in information security and crowdsourcing literature streams. First, the security literature discusses vulnerability management in which the external identifier is only one player (e.g., see Kannan and Telang 2005, Cavusoglu et al. 2007). However, examining a group of security researchers helps us reveal different dynamics where the efficiency distribution and the total number can substantially affect the decisions in a BBP. Second, our model captures several characteristics of BBPs, including the bounty's PR effect, which is a departure from the crowdsourcing literature where the goal of setting reward is to elicit better performance from participants (e.g., see Terwiesch and Xu 2008, Körpeoğlu and Cho 2018). In particular, our modeling approach enables us to show that the PR effect plays a subtle role in affecting an organization's strategies in responding to increased productivity levels or the number of security researchers.

Equilibrium total cost.

The previous section highlights the importance of how security researcher-centric measures, such as their productivity levels and the size of the crowd, impact the de-

cisions of the organization in setting up the bounty. Although the heterogeneity in the productivity levels of security researchers is a debated topic in practice (Lemos 2021), there is a lack of formal analyses on how the total cost is impacted by productivity levels and the heterogeneity therein. Furthermore, no study investigates how the number of security researchers affects the total cost of a BBP. Therefore, we ask the following questions: *Does having an increased level of the lower bound or the upper bounty of security researchers' productivity correspond to a lower total cost of a BBP? Does having a larger crowd imply a lower total cost of a BBP?* We address these questions in Proposition 3.4.3.

Proposition 3.4.3 (i) *It is better to have experts' productivity at an increased level rather than the novices' productivity levels, although the total cost is lower if the lower bound or the upper bound of the productivity level is higher. In other words, $\frac{d\Pi}{d\bar{a}} < \frac{d\Pi}{d\bar{a}} < 0$.*

(ii) *If the number of security researchers (i.e., n) is higher, the total cost of the BBP may interestingly be higher, i.e., $\frac{\partial\Pi}{\partial n} > 0$. This happens if and only if*

(a) *the security researcher heterogeneity is smaller than a threshold, i.e., $\frac{\bar{a}}{a} \leq$*

$$\frac{6n^2-4n+1}{(1-2n)^2}, \text{ or}$$

(b) *the security researcher heterogeneity is larger than the same threshold, i.e.,*

$$\frac{\bar{a}}{a} > \frac{6n^2-4n+1}{(1-2n)^2}, \text{ and the efficiency of PR effect is larger than another thresh-$$

$$\text{old, i.e., } \theta > \hat{\theta}_2 = \frac{\ln\omega c_p((2(7-9n)n-3)\bar{a}-(1-2n)^2(2n-3)\bar{a})}{c_a((-6n^2+4n-1)\bar{a}+(1-2n)^2\bar{a})(\beta\omega+T)} + \frac{l((n-1)(2n-1)\bar{a}+(3n-1)\bar{a})}{2cn(2n-1)(\beta\omega+T)} +$$

$$\frac{1}{\beta c_a(\beta\omega+T)}.$$

Having higher levels of the lower bound or the upper bound of productivity has the opposite impact on the heterogeneity among the security researchers. Therefore, increasing the upper bound (i.e., having the experts' productivity at a higher level) might be considered more detrimental to the BBP because it implies a higher heterogeneity among the security researchers. In contrast, part (i) of Proposition 3.4.3 reveals that although having higher levels of both of the bounds is beneficial, an increased level of heterogeneity by having the experts more productive corresponds to a

lower total cost for the organization. First, let us explain why the total cost decreases in both bounds. Although more productive security researchers can discover a vulnerability earlier (i.e., $\frac{\partial \mathbb{E}[I^*]}{\partial a} < 0$)⁶, the damage cost does not necessarily decrease. Interestingly, the proof of the proposition suggests that the damage cost may increase in the productivity of security researchers when the efficiency of the PR effect is large (i.e., $\theta > \frac{\sqrt{\beta^2 l^2 c_a^2 ((n-1)(2n-1)\bar{a} + (3n-1)\underline{a})^2 + \Sigma}}{2\beta cn(2n-1)c_a(\beta\omega + T)}$, where $\Sigma = 4c^2(1 - 2n)^2 n^2 (\beta l n \omega c_p + 1)^2$). Furthermore, the bounty cost and post-discovery cost decrease (i.e., $\frac{\partial b^*}{\partial a} < 0$ and $\frac{\partial K^*}{\partial a} > 0$) since the organization may lower the bounty because of the higher productivity of security researchers as Proposition 3.4.2 implies. The proof of Proposition 3.4.3 suggests that these reductions in cost are always larger than the magnitude of increase in the total damage cost. Therefore, the total cost of the BBP decreases. On the other hand, if the damage cost decreases in the productivity of security researchers (i.e., when $\theta \leq \frac{\sqrt{\beta^2 l^2 c_a^2 ((n-1)(2n-1)\bar{a} + (3n-1)\underline{a})^2 + \Sigma}}{2\beta cn(2n-1)c_a(\beta\omega + T)}$, where $\Sigma = 4c^2(1 - 2n)^2 n^2 (\beta l n \omega c_p + 1)^2$), the organization increases the bounty and incurs a higher bounty cost and post-discovery cost as implied by Proposition 3.4.2. However, the magnitude of reduction in the damage cost outweighs the magnitude of increase in other costs. Therefore, increasing security researchers' productivity lowers the total cost of the BBP in either case.

In part (i) of the proposition, let us now explain why having a higher productivity level of experts is more beneficial to the organization compared to that of the novices (i.e., $\frac{\partial \Pi}{\partial \underline{a}} > \frac{\partial \Pi}{\partial \bar{a}}$) although more productive experts imply a higher level of heterogeneity across the security researchers. This is because the changes in all cost terms are more sensitive to the productivity of experts (e.g., $|\frac{\partial b^*}{\partial a}| < |\frac{\partial b^*}{\partial \bar{a}}|$) since experts' effort can drive a larger magnitude of reduction in the vulnerability discovery time (i.e., $|\frac{\partial \mathbb{E}[I]}{\partial \underline{a}}| < |\frac{\partial \mathbb{E}[I]}{\partial \bar{a}}|$). If the efficiency of PR effect is large, although the total damage cost is positively associated with productivity (i.e., $\frac{\partial \mathbb{E}[D^*]}{\partial a} > 0$), the proof reveals that experts of higher productivity can drive a substantial reduction in the bounty cost and post-discovery cost to offset a larger magnitude of the increased damage cost comparing to novices of higher productivity. In other words, $|\frac{\partial(b^* + K^*)}{\partial \bar{a}}| - |\frac{\partial \mathbb{E}[D^*]}{\partial \bar{a}}| > |\frac{\partial(b^* + K^*)}{\partial \underline{a}}| - |\frac{\partial \mathbb{E}[D^*]}{\partial \underline{a}}|$. On the other hand, if the PR effect is small, then the damage cost decreases

⁶We use a to denote both \underline{a} and \bar{a} for brevity if the results apply with both of these bounds.

in productivity of security researchers (i.e., $\frac{\partial \mathbb{E}[D^*]}{\partial a} < 0$). In this case, experts of higher productivity can drive a substantial reduction in the damage cost and offset the increased bounty and post-discovery costs more effectively. In other words, $|\frac{\partial \mathbb{E}[D^*]}{\partial \bar{a}}| - |\frac{\partial(b^*+K^*)}{\partial \bar{a}}| > |\frac{\partial \mathbb{E}[D^*]}{\partial \bar{a}}| - |\frac{\partial(b^*+K^*)}{\partial \bar{a}}|$. As a result, having experts' productivity higher is more effective in lowering the total cost than those of novices.

Next, we analyze part (ii) of the proposition. Having an open crowdsourcing program or involving a larger number of participants is shown to help achieve better performance measures for certain tasks in different contexts (e.g., see Terwiesch and Xu 2008, Körpeoğlu and Cho 2018). However, our results reveal some nuances in the context of BBPs. Specifically, involving a larger number of security researchers may sometimes lower the cost-effectiveness of a BBP. It happens in two cases. First, if the heterogeneity of the productivity of security researchers is low (i.e., $\frac{\bar{a}}{a} \leq \frac{6n^2-4n+1}{(1-2n)^2}$), security researchers are similar to each other in terms of productivity. Therefore, the competition among security researchers is high, and the larger number of participants only exacerbates this competition. It results in inefficiencies in the BBP and increases the total cost. In the second case, when the heterogeneity among security researchers is high (i.e., $\frac{\bar{a}}{a} > \frac{6n^2-4n+1}{(1-2n)^2}$) and the efficiency of the PR effect is also large (i.e., $\theta > \hat{\theta}_2$), having a high number of security researchers is also not beneficial to the organization (i.e., $\frac{\partial \mathbb{E}[\Pi^*]}{\partial n} > 0$) because the post-discovery cost prohibitively increases as the number of security researchers increase. Figure 3.2 illustrate the part (ii) of Proposition 3.4.3.

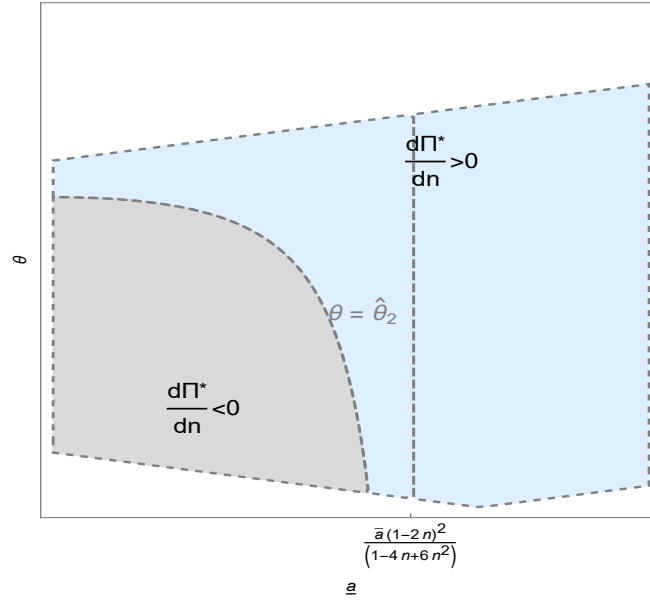


Figure 3.2. The Marginal Effect of an Additional Security Researchers on the Equilibrium Total Cost as a Function of Productivity Heterogeneity $\frac{\bar{a}}{a}$ and PR Effect θ

Propositions 3.4.3 first shed light on how security researchers' productivity levels affect a BBP's cost-effectiveness. Although a higher productivity level of security researchers does not always lower the damage cost, which is in contrast to the expectations in practice (e.g., see Harrington 2021), interestingly, it always decreases the total cost of a BBP. The results justify the prevalence of hacking tutorials and testing software provided in many BBPs (Bugcrowd 2017, Hackerone 2019). Those productivity-enhancing tools can improve a BBP's cost-effectiveness. Nevertheless, we also found that it would be more effective to enhance experts' productivity than novices' productivity. Therefore, organizations need to consider providing advanced tools geared toward security experts. For example, the release of technical details of similar vulnerabilities or the focal organization's IT infrastructure reveals some "deep features," which can be better leveraged by security experts to increase productivity (Giboney et al. 2016).

Furthermore, organizations face tradeoffs in having a smaller or larger number of security researchers participating in their BBPs in practice. Our findings in Proposition 3.4.3 suggest that a higher number of security researchers may not be beneficial

when the heterogeneity of the productivity of security researchers is not large. This is actually observed in practice when a BBP attracts security researchers of similar productivity, for example, when the BBP targets vulnerabilities that are easier to discover, such as cross-site scripting (XSS) vulnerabilities (Owens 2018). Therefore, a smaller group of security researchers is more beneficial in a BBP if an organization engages with security researchers with low heterogeneity in productivity. Even if the heterogeneity is high, the organization should consider another impact of the bounty - the PR effect. If the PR effect is pronounced, the organization may be better off with a smaller group of security researchers in its BBP.

We contribute to the literature on crowdsourcing. Our models and results depart from the literature in several ways. First, we are the first to formally analyze how characteristics of security researchers (such as their heterogeneity) affect the total of BBPs, while security literature mainly focuses on the damage cost of a certain investment (e.g., Lee et al. 2016).

Furthermore, we explore how the number of security researchers affects the total cost of BBPs, which has not been examined in the literature. Lastly, our results capture the interaction between characteristics of security researchers and a substitutive effect of bounty (PR effect) and how this interaction impacts the total costs, illustrating the unique factors in the BBP contexts.

3.4.3 How Does Legal Protection Impact the Bounty and Total Cost?

In this section, we investigate how the legal protection offered to participants in the BBP impacts the bounty and the total cost. As discussed before, a BBP does not guarantee that the security researcher that identifies the vulnerability earliest will be rewarded the bounty. This issue is one of the most debated topics in the BBP domain (Park and Albert 2020, Haworth 2021). In effect, the legal protection offered to the BBP participants adjusts the security researchers' beliefs that they will indeed receive the bounty even if they are the first to discover the vulnerability. Hence, on

the one hand, the lack of legal protections may discourage security researchers from exerting high levels of effort.

Although some BBPs have certain policies to mitigate this issue, the legal scope is ambiguous (Elazari 2018). On the other hand, offering full protection for security researchers may impose threats to the organization after the vulnerability is discovered (Neumann and Hudson 2021). For instance, a security researcher discovered a vulnerability in Foxit’s PDF reader and then decided to expose the zero-day vulnerability ahead of a standard 120-day response disclosure limit (Bisson 2017).

Recently, some security professionals advocate establishing “safe harbor” for security researchers, suggesting that it would be beneficial to protect security researchers (e.g., Lynch 2021, Osborne 2018). Although these issues have been debated in practice, to our knowledge, there is no formal that investigates this issue. Therefore, we examine how an organization’s decisions and total costs are impacted by the legal regime, which is generally set by legal bodies or industrial context (Pfefferkorn 2020). More specifically, we ask the following questions: *Does a higher level of legal protection for security researchers correspond to a lower bounty? Furthermore, does the practice imply an increased total cost of a BBP?* These questions are addressed in Proposition 3.4.4 below.

Proposition 3.4.4 *If the level of legal protection for security researchers (i.e., l) is higher:*

- (i) *The organization may need to have a higher bounty iff the unit damage cost is smaller than a threshold. In other words, $\frac{\partial b}{\partial l} > 0$ iff $c_a < \frac{1}{\beta\theta(\beta\omega+T)}$.*
- (ii) *The total cost of the BBP may be lower. This happens iff the unit post-discovery cost is smaller than a threshold. In other words, $\frac{\partial \Pi}{\partial l} < 0$ iff $c_p < \hat{c}_{p1} = \frac{c_a((n-1)\bar{a} + \frac{a-3n\bar{a}}{1-2n})}{2cn^2\omega} - \frac{\beta\theta c_a(\beta\omega+T)-1}{\beta l n\omega}$.*

Let us first explain part (i) of Proposition 3.4.4. Because the level of legal protection incentivizes the security researchers to exert more effort, one might expect that a higher level of legal protection corresponds to a lower bounty. However, Proposition 3.4.4 implies that it is not necessarily the case. This result can be explained

based on the direct and indirect impacts of legal protection on the damage cost and the post-discovery cost. First, if security researchers have a higher level of legal protection, the organization experiences higher risks of having post-discovery incidents, which increases the marginal effect of bounty in increasing post-discovery cost, i.e., $\left|\frac{\partial K}{\partial b}\right|$ increases in l . Second, increasing the level of legal protection induces an increase in the marginal effect of a bounty in lowering the total damage cost, i.e., $\left|\frac{\partial D}{\partial b}\right|$ increases in l . Furthermore, Lemmas 3.3.1 and 3.3.2 imply that a higher level of legal protection leads to an better incentive posture of the BBP, i.e., $\frac{\partial^2 c_i}{\partial b \partial l} > 0$, ceteris paribus. This further implies that the marginal impact of the bounty on the earliest discovery time is also higher if the level of legal protection is more, i.e., $\frac{\partial \left|\frac{\partial l}{\partial b}\right|}{\partial l} > 0$. However, Lemma 3.3.2 implies that the bounty increases in the unit damage cost, i.e., $\frac{db^*}{dc_a} > 0$. Therefore, if the unit damage cost is small enough, i.e., if $c_a < \frac{1}{\beta\theta(\beta\omega+T)}$, then increasing the level of legal protection induces a greater increase in the marginal effect of the bounty in lowering the total damage cost compared to the first effect on the post-discovery cost, i.e., $\frac{\partial \left|\frac{\partial D}{\partial b}\right|}{\partial l} > \frac{\partial \left|\frac{\partial K}{\partial b}\right|}{\partial l}$. Therefore, the equilibrium bounty increases in the level of legal protection if the unit damage cost is low. The results can be explained similarly for the case when $c_a > \frac{1}{\beta\theta(\beta\omega+T)}$. In this case, the bounty is higher if the level of legal protection is higher. We omit a detailed discussion for brevity.

We now explain part (ii) of Proposition 3.4.4. Many organizations have concerns that legal protection for security researchers may bring in additional costs since security researchers may disclose the vulnerability that we capture in our model with the post-discovery cost. Therefore, one may think that when legal protection for security researchers (i.e., l) is higher, the total cost of the BBP increases. However, part (ii) of Proposition 3.4.4 indicates that it is not always the case. This result is due to the level of legal protection's three different impacts on the cost terms: (i) damage cost, (ii) post-discovery cost, and (ii) cost of the bounty itself. As discussed before, first, the level of legal protection lowers the damage cost - because the security researchers are incentivized to work harder and find the vulnerability earlier. Second, a higher level of legal protection has a higher post-discovery cost - because the security researchers are more relaxed to leak the vulnerability. Third, as part (i) of Proposition 3.4.4 suggests,

the bounty may increase or decrease with the level of legal protection depending on the unit damage cost (i.e., c_a). Furthermore, it is clear that the first two costs depend on the unit damage cost (i.e., c_a) and the unit post-discovery cost (i.e., c_p). The proof of the Proposition 3.4.4 reveals that if the unit post-discovery cost is lower than a threshold (i.e. $c_p < \hat{c}_{p1}$), the total cost is actually lower with a higher level of legal protection. This condition can be rewritten as $\frac{c_p}{c_a} + \frac{1}{c_a} \frac{1}{\beta n \omega} < \frac{(n-1)\bar{a} + \frac{a-3na}{1-2n}}{2cn^2\omega} - \frac{\theta(\beta\omega+T)}{ln\omega}$. This implies that if the relative importance of damage cost is high compared to the post-discovery cost (i.e., $\frac{c_p}{c_a}$ is low), then the total cost decreases in the level of legal protection.

These results yield several practical implications. Legal uncertainties are salient in BBPs as security researchers might be disincentivized if they do not believe that they will be awarded the bounty because of legal issues (Gamero-Garrido et al. 2017). An increasing number of security practitioners advocate that authorities or agencies should legally protect security researchers in doing BBP related tasks. Many industries have established standards to protect security researchers' rights and efforts (Lynch 2021). Contrary to the perception that a higher level of legal protection increases the total cost of the BBP, it is also possible to have the total cost decrease in the level of legal protection. It is interesting to note, if the level of legal protection is higher, that the change in the bounty depends on the unit damage cost, whereas the total cost depends on the ratio of the unit post-discovery cost and damage costs. Therefore, the managers and the policymakers should pay attention to these cost terms. It is imperative as the post-discovery cost is sometimes overlooked in practice (Neumann and Hudson 2021).

Although legal protection is one of the topics debated in the literature (Gamero-Garrido et al. 2017), there is no prior work in the literature that considers this effect. With Proposition 3.4.4, we fill this gap in the literature by examining how legal protection offered to security researchers impacts the dynamics and cost structure of BBPs.

3.5 Extensions

3.5.1 Strategic Hacker

In this extension, we consider a strategic hacker who can observe the BBP when making attacking decisions. Therefore, after an organization announces a bounty, a group of security researchers and a strategic hacker decide simultaneously. The hacker searches for the vulnerability and leverages it to benefit from malicious attacks. The hacker determines the level of effort (i.e., e_h) to maximize the total payoffs in exploiting the vulnerability.

For the strategic hacker, the benefits of vulnerability exploitation are determined by (i) the base level of profits and (ii) the exploitation duration. We consider the base level of profits for the hacker is r_h . The exploitation duration is the time windows between two time points: the time when a strategic hacker identifies the vulnerability and the time when the vulnerability is fixed.⁷ The strategic hacker exerts efforts (i.e., e_h) to discover the vulnerability. Similar to security researchers, the hacker's performance is $a_h e_h$ where a_h is the hacker's productivity. Therefore, the hacker's discovery time is $T - a_h e_h$. The time when the vulnerability is fixed is also the vulnerability's lifecycle (i.e., $\mathbb{E}[L] = \mathbb{E}[I] + \beta\omega$). Therefore the exploitation duration can be written as $\mathbb{E}[I + \beta\omega] - T + a_h e_h$.

Furthermore, the hacker incurs a cost (i.e., γ) per unit effort. Hence the total cost is $\gamma * e_h$. Considering all the dynamics, the total payoffs of the hacker is

$$\mathbb{E}[\Pi_h] = \int_{T-a_h e_h}^{\mathbb{E}[I]+\beta\omega} r_h dt - \gamma e_h.$$

Similar to the damage cost, we consider that the base level of the damage cost caused by the strategic hacker \hat{c}_h is i.i.d. and follows a general distribution Λ_h . As a result, the mean (i.e., $\int_{\Lambda_h} \hat{c}_h dx$) of this parameter with c_h and use it in the analysis hereafter as the unit damage cost caused by the strategic hacker. Therefore, the organization's objective function can be written as:

⁷Some organizations use workarounds instead of applying full patches (higher quality of remediation) to stop the vulnerability from being exploited (Arora et al. 2008), we consider workarounds are patches since the quality of remediation can be represented by c_h in our model.

$$\min_b \mathbb{E}[\Pi] = b + \int_0^{\mathbb{E}[I]+\omega\beta} c_a\beta(1-\theta b) dt + \int_{T-a_h e_h}^{\mathbb{E}[I]+\omega\beta} c_h\beta(1-\theta b) dt + \int_{\mathbb{E}[I]}^{\mathbb{E}[I]+\omega\beta} c_p b n l dt.$$

Our proofs in the Appendix show that the key results are qualitatively similar to those in the main model.

3.5.2 Endogenize Organization's Security Posture

For most organizations whose main businesses are not providing IT services, increasing the security posture during a short-term horizon is not a feasible solution. It is because hiring IT security staff that can understand the inner workings of the software application or infrastructure is generally a long-term endeavor (Petersen 2019). Therefore, our model considers that an organization's security posture is constant. Nevertheless, some organizations have slack resources in controlling IT security, such as software vendors or IT services providers. Hence they can allocate resources to information security at their discretion. To examine their strategies and payoffs in BBPs, we consider the case when the organization can decide its security postures in the game. Therefore, the cost coefficient of improving security posture is ζ . We use a quadratic cost structure since it is extremely to reach perfect security. Therefore the total investment an organization makes in establishing security posture is $(1-\beta)^2\zeta$. The question can be written as follow:

$$\min_{b,\beta} \mathbb{E}[\Pi] = b + \int_0^{\mathbb{E}[I]+\omega\beta} c_a\beta(1-\theta b) dt + \int_{\mathbb{E}[I]}^{\mathbb{E}[I]+\omega\beta} c_p b n l dt + (1-\beta)^2\zeta \quad (3.2)$$

According to the proof in the Appendix, our key findings still hold qualitatively.

3.5.3 Multiple Vulnerabilities

As discussed before, security researchers' experience, in general, is limited (Votipka et al. 2018). Therefore, each is dedicated to finding "the" vulnerability she is most apt to find (Votipka et al. 2018). Therefore, in our main model, we consider one vulnerability in the BBP, which is also in line with the literature (e.g., Arora et al.

2008, Kannan and Telang 2005). For robustness, we now examine the case when there are multiple (i.e., M) vulnerabilities in the BBP’s targeted information system that could each be identified by independent groups of security researchers.⁸

Specifically, a group (with index m) of security researcher with heterogeneous efficiency (i.e., $c_i^m \sim U(\underline{c}^m, \bar{c}^m)$) can find one particular vulnerability (i.e., vulnerability m). Similarly, the earliest discovery time, post-discovery cost, and patching complexity for each vulnerability m is $\mathbb{E}[I^m]$, ω^m , and c_p^m , respectively. Then the organization needs to decide a bounty (i.e., b^m) for each vulnerability m . We derive solutions and provide details in the proof in the Appendix. The results suggest that all our key results are qualitatively the same.

3.6 Discussion and Conclusion

The future of cybersecurity will require more collaboration from the community of security researchers and organizations. In 2018, the National Institute of Standard and Technology (NIST) added “coordinated vulnerability disclosure life-cycle” as a core practice in the cybersecurity framework (NIST 2018). It highlights that organizations should be more open to external security researchers and adjust their strategies in vulnerability management accordingly. To effectively take advantage of BBPs, it is imperative for organizations to gain a better understanding of the crowd-sourced security solution in terms of benefits and costs. In particular, characteristics of security researchers, organizations, and legal protection for security researchers need to be considered when launching BBPs.

3.6.1 Practical Implications for Bounty Design

First, we examine the role of organizations’ security features, including the patching complexity and the security posture, in affecting the optimal bounty. Interestingly,

⁸Note that the model can also be developed based on dependencies on vulnerabilities or security researchers. However, the results are qualitatively similar, although the solutions and the discussion are lengthy. Hence, we skip a detailed discussion for brevity.

if patching a vulnerability is of high complexity, the organization may need to lower the bounty if it has a high level of security posture. Nevertheless, an organization of low security posture should always increase the bounty. This shows that BBP can be an substitute for an organization's in-house vulnerability management.

Furthermore, we investigate how the characteristics of security researchers, including the productivity level and the total number, affect the optimal bounty. Our analyses reveal that if security researchers gain improvements in their productivity, an organization may need to further increase the bounty if and only if the efficiency of PR effect is low. Therefore, when security researchers access to more effective tools or tutorials (Laszka et al. 2018, Zhang et al. 2015), organizations that suffer more damage costs from operational disruptions (rather than reputation losses) need to increase the bounty to further incentivize the more efficient crowd. When more security researchers participate, the organization may also need to increase the bounty. Interestingly, it happens if the heterogeneity of security researchers' productivity is high but the efficiency of the PR effect is low, or the heterogeneity of security researchers' productivity is low but the efficiency of the PR effect is high. Since a bounty's incentive effect and its PR effect are substitutes, it is important to realize which one is dominate. Additionally, an increased crowd of homogeneous security researchers may even hamper the the vulnerability discovery. In that case, the organization need to increase the bounty only when it can reduces the reputation losses substantially.

In a further step, we examine how the characteristics of security researchers affect the total cost of BBPs. When security researchers become more productive, a BBP's total cost always decreases. The results can justify the common strategies that are used by organizations or BBP platforms in terms of providing free tutorial and tools.⁹ However, a larger crowd of security researcher might not be always beneficial to the organization. If the security researchers are homogeneous in productivity's, a larger number of security researchers induce a higher total cost of a BBP. The results are

⁹see <https://www.bugcrowd.com/hackers/bugcrowd-university>; <https://www.hackerone.com/hackers/hacker101>

resonant with the facts that some BBPs elicit a smaller group of security researchers to work on vulnerabilities.

Lastly, we analyze how security protections for security researchers affect the optimal bounty and the total cost of a BBP. Our results reveals that a higher level of protection for security researchers may even incentivize an organization to offer a higher bounty. This happens if the vulnerability is more severe, and the organization can gain more benefits from security researchers that can make more efforts because of the legal protection. Our results also indicate that offering more legal protections may even lower the total costs of a BBPs if the post-discovery cost is sufficiently low.

These results shed light on how organizations adapt the bounty when the levels of efficiency of security researchers change, which is a missing piece in both crowd-sourcing and vulnerability management literature streams. Furthermore, we examine several alternative business settings such as (i) considering a strategic hacker, (ii) endogenous organizational security posture, and (iii) considering multiple vulnerabilities. We find that in these alternative business settings, the key results discussed in our main model are qualitatively the same, suggesting the robustness of our findings.

3.6.2 Future Research Opportunities

There are several research opportunities in the bug bounty setting we investigate. Future research can empirically examine the benefits and costs of BBPs not only to the organization but to the business partners of the organization as well. To the best of our knowledge, there is no prior work investigating the spillover effects in BBPs. Furthermore, future studies can explore the financial returns of BBPs to the organizations based on the types of vulnerabilities identified in the BBPs.

CHAPTER 4
PEER DATA BREACHES AND CYBER RISK
DISCLOSURE QUALITY: EVIDENCE FROM U.S.
PUBLIC FIRMS

Abstract

Public firms' cyber risk disclosure (CRD) is valuable in reducing information asymmetry in the financial market. However, there is limited understanding of whether and how peers' data breach incidents affect a firm's cyber risk disclosure(CRD) quality. To explore the question, we leverage textual data on more than 3,000 US public firms' CRD from 2011 to 2017 and perform empirical analyses. We find that firms strategically lower their CRD quality after peer breaches. The result is robust to instrumental variable analysis, different model specifications, and alternative measurements. We further show that the quality of CRD decreases at a larger magnitude if a firm has more business sites, owns intangible assets of greater value, or if public attention to data breaches is higher. Besides, if a firm invests more in cybersecurity or has higher analyst coverage, the magnitude of reduction in their CRD quality is smaller. We discuss the implications for research and practices.

4.1 Introduction

In the digital age, cyber risks are generally believed to impose substantial threats to firms. However, the information on firms' security posture is limited. The issue has long been a concern from an economic view of cybersecurity as information asymmetry may hinder efficient resources allocations and cause adverse selections (Moore 2010, Schneier 2007). In March 2022, the U.S. Securities and Exchange Commission (SEC) proposed rule changes that intended to enhance disclosures about cybersecurity risk

management by public companies. Although the issue is well recognized, there is little understanding of how firms decide on their voluntary cyber risk disclosure, especially when confronting their peers' data breaches.

While many studies present peer effects in disclosure decisions (Seo 2021), the impact of peer data breach incidents on firms' voluntary cyber risk disclosure has seldom been discussed. Firms' adverse incidents will likely change the external information environment, triggering broad concerns over an entire industry and increasing litigation costs. Consequently, the market will be more skeptical about other firms that provide similar products or services, which is called the "contagion effect" (Kelton and Pennington 2020). Similarly, many high-profile cyber incidents inform investors of idiosyncratic risks and potential losses in certain services or products. In December 2020, a SolarWinds product was found to contain a backdoor for illegal access. The security issues affected 18,000 customers, including Fortune 500 and government agencies (Turton and Bloomberg 2020). As a result, SolarWinds experienced a 23% fall in its stock after disclosing the incident (Novet 2020). Furthermore, the incident arouses the public's attention to the software industry. However, it is unclear how this type of incident impact peer firms' decisions to disclose their cyber risks voluntarily.

This question on peer breaches and cyber risk disclosures has become salient in recent years. First, the visibility and publicity of cyber incidents grow significantly because of the enforcement of mandatory data breach notifications. Until 2020, all 50 states in the US have passed data breach notification laws (NCSL 2021). Furthermore, the EU implemented General Data Protection Regulation (GDPR) in 2018 and enforced a 72-hour data breach notification deadline (Nieuwesteeg and Faure 2018). These laws publicize related incidents, potentially increasing the litigation costs of violating data security or privacy and causing spillover effects. Under these circumstances, firms are more likely to react to peers' breaches. Second, cyber risk disclosure is under increasing scrutiny. To improve transparency about public firms' security postures, the US Securities and Exchange Commission (SEC) published guidance on cyber disclosure in 2011 and updated it in 2018. In June 2021, the SEC announced that it would focus on cybersecurity disclosures made by public companies as part of

its regulatory agenda.¹ In 2022, the SEC proposed rules that intended to substantially impact how firms and management report cyber incidents and cybersecurity oversight (Wolfman et al. 2022).

Although the values of cyber risk disclosure are well recognized, many criticize that most disclosures might not be informative to market participants since they are generic and qualitative. The 2011 SEC cyber disclosure guidance emphasizes that firms need to provide disclosure “tailored to their particular circumstances” (SEC 2011). For one thing, there is no mandatory or specific requirement about the contents or lengths of the disclosure. Furthermore, high uncertainties of cyber risks make it difficult for managers to assess and describe their cybersecurity. As a result, many firms tend to disclose all possible risks to lower potential litigation costs, which makes the disclosure limited to investors. However, data breaches make the risks and contingent losses more visible to the public, which is likely to affect the disclosure pattern of firms that are facing similar threats. Understanding firms’ incentives in disclosing cyber risk in response to peer breaches has nontrivial theoretical and policy implications. Therefore, we ask: *How does a firm strategically change its cyber risk disclosures (CRD) quality in response to peer breaches?*

The answer to the question is not straightforward. According to the rational disclosure theory (Verrecchia 1983), managers consider both benefits and costs when deciding on disclosures. Nevertheless, how peer breaches affect the perceived payoffs of disclosing cyber risks is seldom investigated. In our context, on the one hand, peer breach may increase the cost of CRD because both focal firms and other market participants would become more sensitive to cyber risks after observing realized breach incidents. Considering that CRD may increase cyber risks and adverse negative market responses, focal firms may tend to release obfuscated or low-quality cyber risk disclosure. On the other hand, the benefits of CRD may also increase because of peer breaches. The main reason is that the focal firm may want to provide higher quality disclosure to differentiate themselves from “low cyber performance” peers.

¹<https://www.sec.gov/news/press-release/2021-99>

Given these countervailing forces, the net effect of peer breaches on CRD quality is an empirical question.

To analyze the question, we construct a proxy for CRD quality by leveraging rich textual data from public firms' financial filings from 2011 to 2017. Next, we compile an innovative dataset covering firms' comprehensive characteristics, including financial performance, auditing information, and information technology adoptions. Lastly, we carefully address endogeneity concerns in analyses. While peer breaches are plausibly exogenous to focal firms' propensity to disclose cyber risks, unobserved shifts in industries and legal regimes may affect peer breaches and CRD tendency. In order to tackle the issue, we leverage several identification strategies such as instrumental variables.

Our findings reveal that firms strategically lower the CRD quality after peer breaches. The result is robust to different specifications, alternative measurements, and 2SLS estimations with instruments. Furthermore, the CRD quality decreases at a larger magnitude when firms have more sites or own more intangible assets. In addition, the level of public attention to cyber risks and firms' reliance on customer markets exacerbates the decrease in CRD quality after peer breaches. This study complements the economics of information security and corporate disclosure literature. Additionally, a firm provides longer cyber risk disclosure in response to peer breaches. Lastly, the decline in disclosure quality is smaller when a firm invests more in cybersecurity or has high analyst coverage. The findings provide practical implications for stakeholders, public firms, and policymakers.

4.2 Literature Review

Our study is related to three streams of literature, including 1) impacts of IT security incidents; 2) industry peers; 3) voluntary disclosure incentives.

4.2.1 Impacts of IT Security Incidents

Information Systems studies extensively examine how IT security incidents affect a firm's financial performance and what strategic actions it takes to mitigate negative consequences. Many argue that firms that experienced cyber incidents suffered negative consequences, including drops in stock prices (Telang and Wattal 2007), reputation damages (Tanimura and Wehrly 2015), and decreases in consumer spending (Janakiraman et al. 2018). Furthermore, the extent of negative consequences is affected by characteristics of breach incidents, firms, and customers (Martin et al. 2017). In order to mitigate the negative impact, firms strategically respond to data breach incidents in various ways. Previous studies suggest data breach announcements occur on days when media is expected to be busy, which suggests breached firms leverage strategic timing (Foerderer and Schuetz 2022). Furthermore, breached firms tend to increase investment in IT security countermeasures such as hiring more security experts (Bana et al. 2021) and spending more on advertising to rebuild reputations (Choi and Johnson 2019).

Our study complements the literature by investigating the impact of peer breaches on firms' voluntary cyber risk disclosure. There is evidence that managers are aware of peer breaches and take specific actions to reduce future cyber risks (Bana et al. 2021). Although peer breaches do not directly affect focal firms' operations, managers can observe that peers experience substantial loss (e.g., degraded reputation, lower stock price) caused by security breaches. Therefore, they are more likely to allocate resources to security, which is a known spillover effect of breach incidents. Nevertheless, it is intriguing how peer breaches affect firms' narratives about their cyber risks. In particular, it is unclear how managers perceive markets' response to their cyber risk disclosure when cyber threats are manifest. Our study sheds light on the issue and fills the literature gap by examining the net effect of peer breaches and investigating the underlying mechanisms.

4.2.2 Industry Peers

Firms have incentives to examine what happened to their peers and adopt strategic actions in response to their peers' actions or events (Ashraf 2021, He et al. 2018, Krieger 2021). It is mainly because that firms within the same industry have similar supply and demand conditions, investment opportunities, and sensitivity to exogenous influences like regulations (Rogers et al. 2014). Furthermore, peer firms have intensive interactions because of the competitive environments (Aghamolla and Thakor 2022). Therefore, peer-relevant information can be helpful for focal firms in terms of lowering environmental uncertainties (Seo 2021).

Our study is closely related to peers' negative incidents, which pose interesting tensions regarding its spillover effect. For one thing, the negative spillover effect may hurt the focal firm because market participants become more pessimistic about similar firms' performance (Kelton and Pennington 2020). For another thing, focal firms may benefit from the competitive effect when peers are losing their market shares (Cao et al. 2021). Previous studies demonstrate that firms take various measures in response to their peers' negative incidents. For instance, firms adjust marketing strategies if their peers experience product-harm crises (Cao et al. 2021, He et al. 2018). In addition, firms abandon their R&D projects in response to their peers' failure if they are in the market of the same customer and technology (Krieger 2021).

Similarly, when a firm's peer experiences a data breach incident, the firm may rationally anticipate increased scrutiny from market participants. However, cyber risks are different from risks in products and services. First, cybersecurity cannot directly contribute to business values. Therefore, its impacts may not be as substantial as other negative incidents. Second, it has relatively high uncertainty and technical complexity. Besides, firms' strategies to respond to cyber risks might differ from other risks. Recent studies shed light on the impact of peer breaches on firms' IT security investment (Bana et al. 2021) and internal control material weaknesses (Ashraf 2021). They present that firms may learn from peers' failures and try to improve their cyber

resilience. Nevertheless, firms' strategic responses in voluntarily disclosing cyber risks have seldom been rigorously examined. Our study fills in the gap.

4.2.3 Voluntary Disclosure Incentives

Corporate disclosure focus on primary business operations and audited financial performance. It significantly impacts products and the capital market (Beyer et al. 2010). In particular, informative disclosure can reduce information asymmetry and increase market efficiencies (Healy and Palepu 2001, Kot 2009). However, providing informative or high-quality disclosure is not always in the best interest of firms' management.

In effect, managers face trade-offs between the benefits and costs of disclosing information to maximize their firm's market price (Verrecchia 1983, Diamond 1985, Heinle and Smith 2017). On the one hand, firms usually incur non-trivial proprietary costs when they publicize more detailed information about themselves (Teoh and Hwang 1991, Verrecchia 1983). The cost stems from the possibility that the disclosed information may be leveraged by competitors or elicited unwanted regulatory attention (Teoh and Hwang 1991, Park et al. 2019). On the other hand, disclosing detailed and credible information can improve firms' image and enhance the relationship between stakeholders, suppliers, and customers (Skinner 1994, Derouiche et al. 2021). By changing managers' perceptions about the benefits and costs of disclosing information (Lambert et al. 2007, Frenkel et al. 2020), exogenous shocks (i.e., information events) to the information environment can shift firms' voluntary disclosure patterns. Many studies examine how exogenous information related to firms' businesses impacts voluntary disclosure quality (e.g., Anantharaman and Zhang 2011). Nevertheless, peer breaches are different from information events that are commonly investigated because the perceived payoffs of cyber risk disclosures are somewhat unclear.

Previous studies tap into the area and provide evidence that firms can benefit from disclosing their cyber risks. For instance, firms that disclose cyber risks experience

higher stock prices (Gordon et al. 2010) or lower cost of capital (Havakhor et al. 2020). Nevertheless, the antecedent of cybersecurity disclosure has seldom been rigorously examined before. In particular, there is limited understanding of how peers' data breach incidents affect firms' incentives in disclosing information and the underlying mechanisms. One challenge in examining the question is that there is no standard metric to evaluate their risks. Therefore, we follow previous practices and leverage textual characteristics. Our research setting is similar to Ashraf (2021) in incorporating peer breaches and disclosure quality. However, our paper focuses more on the impact of peer breaches on the disclosure incentives, while Ashraf (2021) mainly use peer breach incidents as identification strategies. Furthermore, we consider internal and external factors to shed light on mechanisms of unintended consequences of data breach incidents.

4.3 Background and Conceptual Model

Cyber risk disclosure (CRD) has become an increasingly important part of voluntary corporate disclosures. In 2005, the SEC mandated all public firms to disclose the "most significant factors make the company speculative or risky" (Regulation S-K, Item 305(c), SEC 2005). The regulation also requires a concise explanation of the risk that is specific to the firm. In 2011 and 2018, SEC introduced and then updated cybersecurity guidelines. Although a few studies reveal that CRD has significant predictive power of cybersecurity risks (Florakis et al. 2020, Wang et al. 2013), many criticize that CRD is not sufficiently helpful to investors since they are generic and qualitative (Cheong et al. 2021, Hilary et al. 2016, Mont 2015). For instance, firms can disclose all possible risks and uncertainties that can be generalized to other firms, which limits CRD's informativeness. As one type of voluntary disclosure, the extent to which firms disclose their cyber risks is at managers' discretion. In other words, managers can decide the optimal level of CRD depending on its payoffs given the available information. Peer breaches serve as key information events that are likely to affect the payoffs of CRD.

For several reasons, peer firms' data breach incidents are likely to affect focal firms' CRD decisions. First, in many cases, a firm's data breach reveals cyber risks to certain businesses and operations that can be generalized to its peers. For example, Marriott's breach incidents show that hotels' information systems are susceptible to hackers' attacks which may leak enormous sensitive data and cause high losses (Diosi 2022). Hence, the incidents affect Marriott's peers, such as Hyatt which is exposed to similar risks and revamped its cybersecurity programs following Marriott's breach (Kerner 2019). Second, the contingent losses of breach incidents are evident. Breached firms may experience significant adverse market reactions, including decreasing stock prices, total revenue, and credit ratings (Foerderer and Schuetz 2022, Combs 2022). In addition to firms' economic losses, management. Following Target's massive breach that affected up to 110 million people, Target CEO Gregg Steinhafel and CIO Beth Jacob announced their resignation in the aftermath of the data breach (Dignan 2014).

Peer breaches may increase the marginal cost of CRD and incentivize managers to provide lower-quality CRD through two main channels. First, it increases managers' expected breach likelihood of their firms. The general proprietary cost suggests that disclosed information can be leveraged by competitors (Verrecchia 1983). Unlike proprietary cost, the actors who can leverage CRD are attackers, such as criminal organizations and insider threats. High-quality CRD needs to contain a firm's specific IT security weaknesses, cybersecurity governance, and defensive strategies. The information makes it easier for attackers to infiltrate IT systems and may expose a firm to higher threats. Therefore, the cost of CRD is positively associated with managers' concern about cyber risks. After peer breaches, managers become more conservative in disclosing unique cyber risks, leading to a drop in their CRD quality. However, it is possible that peer breaches may not significantly increase managers' concern because the firms' awareness of breach risks is adequately high, or managers consider that the causes of peer breaches are substantially idiosyncratic.

Second, peer breaches increase the market's scrutiny of focal firms' cyber risks, which makes CRD more costly to firms. Since peer firms have similar businesses, operations, and information technology infrastructure, realized breach incidents manifest

weaknesses and vulnerabilities in those similar characteristics (Kamiya et al. 2021). The increased public scrutiny potentially makes the market more pessimistic about the cybersecurity performance of other firms similar to the breached firm. As a result, more specific risk disclosure may signal that a firm is vulnerable to potentially disastrous occurrences that could negatively impact its relationships with stakeholders and hinder performance. Therefore, to managers, the perceived cost of CRD becomes higher due to peer breaches. Nevertheless, peer breaches may also increase the benefits of CRD because of the rivalry spillover effect (Cao et al. 2021). Specifically, CRD can be used to infer the relative security postures of firms in the same industry. If that is the case, a high-quality CRD can demonstrate a firm's accountability to stakeholders and signal that the firm is not only aware of the dangers but also actively working to mitigate them and assure long-term viability. Therefore, managers may provide high-quality CRD in response to peer breaches.

To summarize, peer breaches have opposite effects on firms' incentives in disclosing CRD. Therefore, it is necessary to investigate the net impacts empirically. Next, we discuss the data used in the analyses.

4.4 Data Description

We construct a panel dataset of more than 4,000 firms from 2011 to 2017. The post-2011 period is suitable for our research context for two main reasons. First, firms presumably became fully aware of the importance of cybersecurity disclosure after 2011 when SEC issued the first-ever guidance on it. Second, information on most data breach incidents, including breached firms' names and breached records, went public. In 2011, 90% of US states (excluding Alabama 2018, Florida 2014, Kentucky 2014, New Mexico 2017, and South Dakota) mandated data breach notification laws (NCSL 2011). Our main panel dataset is compiled from multiple sources, including (1) cyber risk disclosures in 10-K filings from the EDGAR system; (2) industry peers' data from the TNIC dataset; (3) data breach incidents from Privacy Rights Clearing House; (4) firms financial and accounting characteristics from Compustat; (5) site-

level IT installation status data from CI database. In Table 4.1, we report descriptive analyses of all main variables. Next, we mainly describe how we construct CRD quality measurements and identify peer breaches.

Table 4.1. Summary Statistics

Variables	Definitions	Source	Mean	S.D.
CRD Quality	The quality of cyber risk disclosure.	10-K	1.04	1.00
CRD Length	The number of words of cyber risks disclosure	10-K	87.56	110.27
No. Peer Breaches	The number of peers have breach.	Privacy Rights Clearinghouse	1.22	2.29
Other Risks Disclosures Length	The number of words in disclosure about other risks.	10-K	7.48	1.84
Has Data Breach This Year	An indicator of whether the focal firm has a data breach.	Privacy Rights Clearinghouse	0.01	0.08
Total Asset	Log(Total asset)	COMPUSTAT	6.44	2.42
Intangible Asset	Log(Intangible asset)	COMPUSTAT	3.38	2.87
Operating Expenses	Log (Operating expenses)	COMPUSTAT	5.51	2.32
Book Value per Share	Log (Book value per share)	COMPUSTAT	2.26	1.56
Employees	The number of employees	COMPUSTAT	8.51	30.14
Market HHI	Market competition	COMPUSTAT	0.29	0.28
Internal Weakness	The number of internal weaknesses	Audit Analytics	0.48	1.16
No. Installed Cybersecurity Apps	The number of installed cyber security apps.	CITDB	0.37	0.32
No. Sites	The number of business sites.	CITDB	2.88	1.67
Public Visibility Data Breach	Google search index of the keyword “data breach”	Google Trend	35.66	16.67

4.4.1 Cyber Risks Disclosure

The SEC’s Corporate Finance Division a guideline in 2011, noting that cyber risk is a risk factor that should be declared by organizations if they are materially exposed to it. The guideline also provides examples of what the SEC believes managers should

be revealing (SEC 2011). Specifically, the guideline suggests that firms' cyber risks disclosure can include (1) how their business or operations bring in material risks and what are the potential consequences; (2) how their outsourcings give risk to risks and how they address those risks; (3) the cyber risks they experienced; (4) risks associated with cyber incidents that may remain undiscovered for a long time; (5) cyber insurance coverage (SEC 2011).

In the US, publicly-traded companies are mandated to annually file a comprehensive report 10-K. Many details about business operations and financial performance are disclosed in different items of the report. As a type of risk, cybersecurity issues are usually discussed in Item 1A Risk Factors of 10-K. To capture how firms disclose their cyber risks, we download all 10-K filings filed between 2011 and 2017 from the EDGAR system. Following previous practices (i.e., Gordon et al. 2010, Havakhor et al. 2020), we use a list of comprehensive cybersecurity keywords to search and extract paragraphs that contain at least one keyword in 10-K Item 1A Risk Factors parts. Table C.2 in Appendix present all keywords. As an example, Figure 4.1 shows the cyber risks disclosure in Target's 2011 10-K and cyber-related keywords. Next, we present relevant descriptive analyses of cyber risk disclosure data.

If we fail to protect the security of personal information about our guests, we could be subject to costly government enforcement actions or private litigation and our reputation could suffer.

The nature of our business involves the receipt and storage of personal information about our guests. If we experience a **data security breach**, we could be exposed to government enforcement actions and private litigation. In addition, our guests could lose confidence in our ability to protect their personal information, which could cause them to discontinue usage of our credit card products, decline to use our pharmacy services, or stop shopping at our stores altogether. Such events could lead to lost future sales and adversely affect our results of operations.

A significant disruption in our computer systems could adversely affect our results of operations.

We rely extensively on our computer systems to manage inventory, process transactions and summarize results. Our systems are subject to damage or interruption from power outages, telecommunications failures, **computer viruses**, **security breaches** and catastrophic events. If our systems are damaged or fail to function properly, we may incur substantial costs to repair or replace them, and may experience loss of critical data and interruptions or delays in our ability to manage inventories or process transactions, which could adversely affect our results of operations.

Figure 4.1. Cyber Risk Disclosure in Target's 2011 10-K

In our data sample, there are 49.0% of observations indicate a firm discloses cyber risks from 2011 to 2017, and there are 53.6% of unique firms disclose cyber risks. Figure 4.2 illustrates that the proportion of firms that disclose cyber risks increased

steadily from 2011 to 2017. The trends suggest that CRD plays an increasingly important role in corporate disclosures. Besides, Figure 4.3 shows that the average length of cyber risk disclosure also increased (i.e., the count of words) from 2011 to 2017. Disclosure length can also indicate the extent to which firms are aware of cyber risk disclosure.

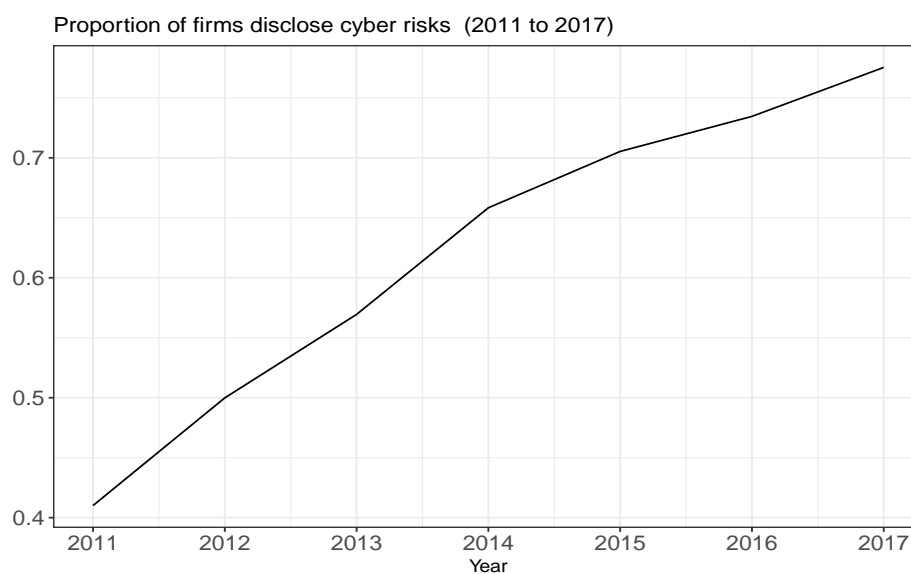


Figure 4.2. Cyber Risk Disclosure Trends - Proportion of Public Firms

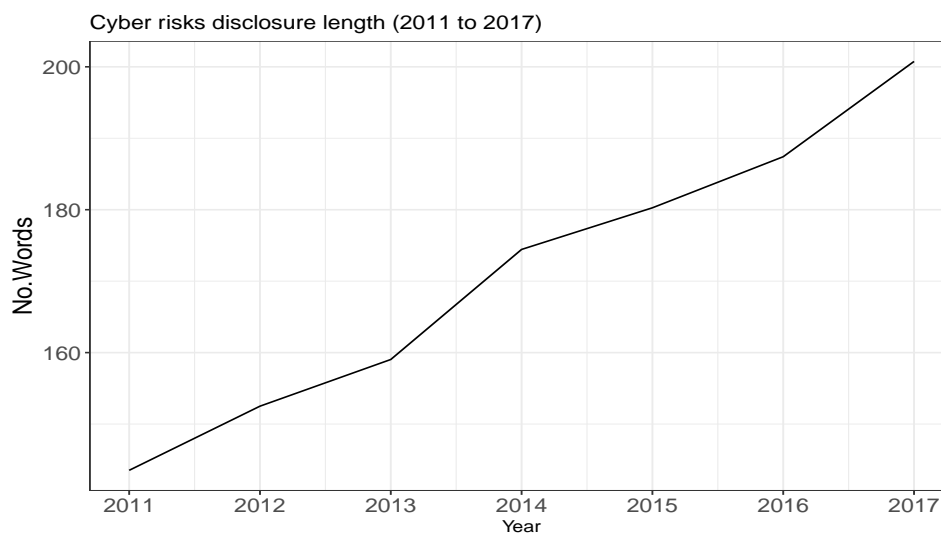


Figure 4.3. Cyber Risk Disclosure Trends - Lengths

4.4.2 Measure Cyber Risks Disclosure Quality

One major challenge in the study is to measure the cyber risks disclosure quality since there is no standard or objective indicator. Based on the complaints about the “lengthy” and “generic” natures of risk disclosure, we focus on the similarity of CRD and use it as a proxy for CRD quality. Specifically, we calculate the average similarity of one firm’s CRD between all other CRDs in the same year. The similarity metrics are also used in previous research (Ashraf 2021, Brown and Tucker 2011). The effectiveness of this measurement is based on three main assumptions. First, CRD could be either generic or specific. For example, firms can either disclose general risks such as unauthorized access or provide more details on how the risks are related to their businesses. Second, it is at the discretion of firms/managers to choose the specific level which may be optimal for them. Third, general security risks may hinder the investors from collecting effective information.

There are three main stages of constructing CRD quality. We first extract cyber risks disclosure content by searching cyber-related keywords in Item 1A Risk Factors of 10-K as mentioned above. In the second stage, we pre-process documents in several ways. In order to capture more informative textual features, we remove stopwords and lemmatize all words. Furthermore, we calculate the weight of each word by using Term Frequency - Inverse Document Frequency (TF-IDF) which can measure the relevance of a term in given documents and is commonly used in textual analyses.

In the last stage, we calculate the similarity between different cyber risk disclosures. To do so, we transport each document into a word vector with TF-IDF weights. Based on all vectors, we can calculate yearly pairwise similarity by using the Cosine similarity metric, which is widely adopted in related tasks (Ashraf 2021, Arora et al. 2021, Pan et al. 2019). The cosine of the angle between two n-dimensional vectors projected in a multi-dimensional space is measured by the cosine similarity metric. We present a brief example of two documents. Two documents each can be represented as vectors - d_1 for document 1 and d_2 for document 2. Therefore,

$d_1 = (w_1, w_2, \dots, w_{n-1}, w_n)$ and $d_2 = (p_1, p_2, \dots, p_{n-1}, p_n)$, where w_i and p_i are counts of each word $i \in [1, n]$. The similarity score is defined as:

$$\text{Similarity} = \cos \theta = \frac{d_1}{\|d_1\|} * \frac{d_2}{\|d_2\|} = \frac{d_1 d_2}{\|d_1\| \|d_2\|},$$

where θ is the angle between d_1 and d_2 , $\|d_1\|$ and $\|d_2\|$ are the vector lengths of d_1 and d_2 , respectively. This value is in the range of 0 and 1. The higher value of *Similarity* suggests a higher similarity between d_1 and d_2 .

Figure 4.4 illustrate the process of measuring CRD similarity. Figure 4.5 shows the wordcloud of high weights words that appears in processed cyber risk disclosure documents. As we can see, the wordcloud highlights several words that are closely related to cyber risks, including “breaches” “data” “access” “technology” “security” and so on. Lastly, we normalized the similarity and use $1 - \text{normalized}(\text{similarity})$ as CRD quality.

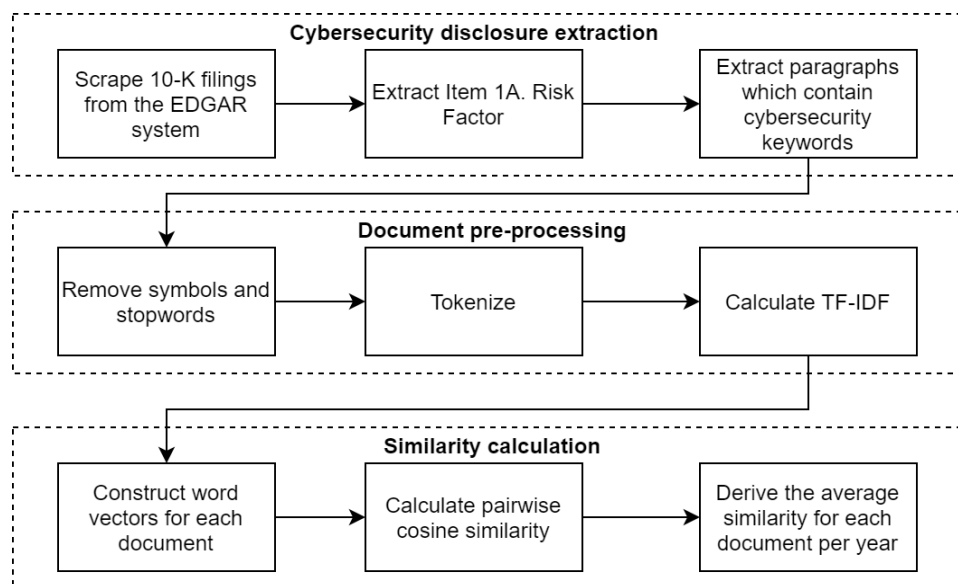


Figure 4.4. The Processes of Measuring Cyber Risk Disclosure Similarities



Figure 4.5. The Wordcloud of Processed Cyber Risks Disclosure Documents based on TF-IDF Weights

4.4.3 Industry Peers' Data Breaches

To obtain information on industry peers' data breaches, we firstly access comprehensive records of data breach incidents from 2011 to 2017 on the Privacy Rights Clearinghouse website. The website has collected and published a list of data breaches that were “confirmed by various sources and/ or notification lists from state government agencies.” The data source is commonly used in other cybersecurity research (Kwon and Johnson 2018, Angst et al. 2017). Figure 4.6 presents the total occurrences of data breaches between 2011 and 2017. Furthermore, Figure 4.7 shows the industries have the highest data breach occurrences each year. It reveals that industries including Finance (insurance and real estate), Manufacturing, Retail Trade, and Services have relatively more data breaches.²

²The industrial classification is based on SIC two-digit codes.

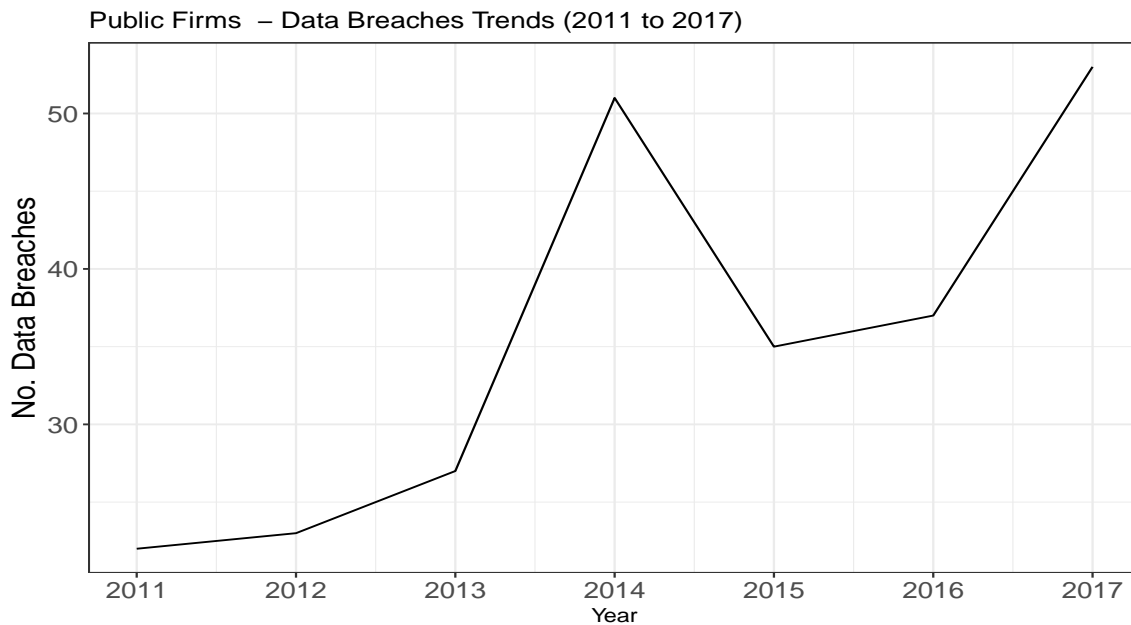


Figure 4.6. Public Firms’ Data Breaches from 2011 to 2017

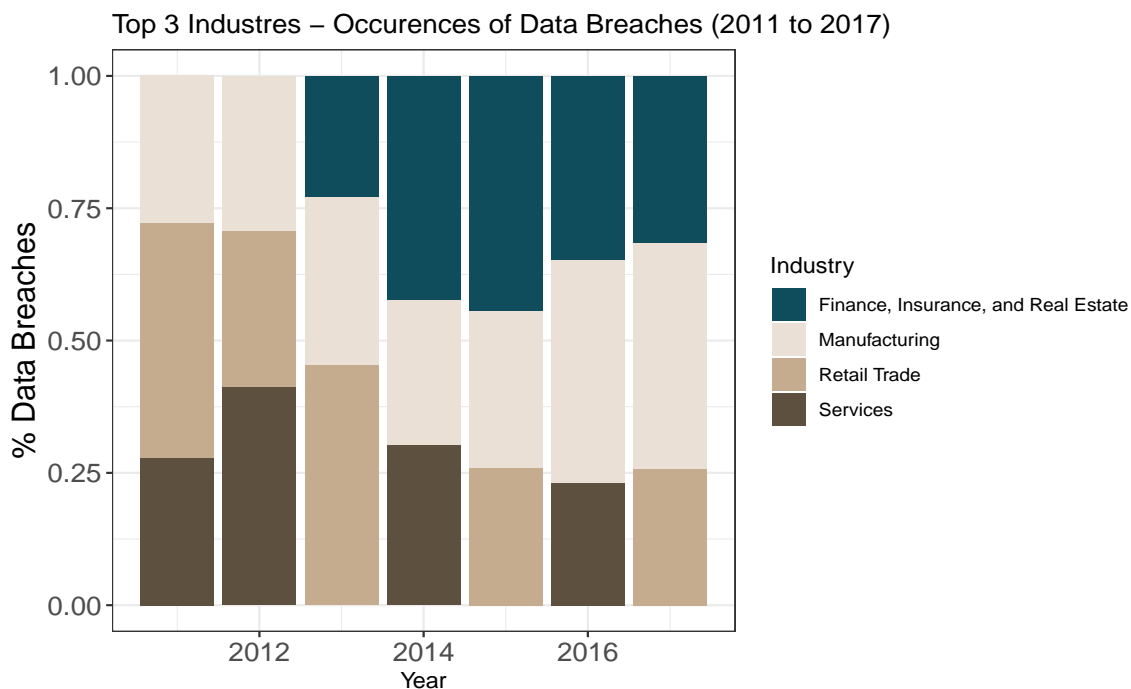


Figure 4.7. Industries and Data Breaches

Next, we capture industry peer relationships using text-based Network Industry Classifications (TNIC) data (Hoberg and Phillips 2016). The data is compiled by a text-based analysis of product descriptions in 10-K filings for each year. Specifically, we leverage the TNIC-3 level (close to the three-digit SIC level) to define industry peers. Unlike industry classification systems like the North American Industry Classification System (NAICS) or the Standard Industrial Classification system (SIC), TNIC can capture the changes in product market similarities annually. This practice allows for more fine-tuned measures of peers whose events and strategies the focal firm might follow closely.

4.5 Main Empirical Analyses

Our main analyses explore how peer breaches affect focal firms' CRD qualities. The primary identifying assumption for the causal inference is that firms may not be able to predict and manipulate the number of peer breach incidents. First, we use OLS and the below model specification as the benchmark model.

$$CRDQuality_{it} = \alpha + \beta No.PeerBreaches_{it} + \gamma ControlVariables_{it} + \mu_i + \tau_t + e_{it}$$

In this model specification, $CRDQuality_{it}$ is a continuous variable which proxy the cyber risks disclosures quality for firm i in year t . $No.PeerBreaches_{it}$ captures the number of peer breaches for firm i in year t . We also capture time-variant control variables $ControlVariables_{it}$, firm fixed effect μ_i , and time fixed effect τ_t .

We present our results in Table 4.2. Columns (1) and (2) present that the number of peer breaches has significantly negatively affects the quality of CRD. Specifically, one additional peer breach leads to a 0.01 standard deviation decrease in the quality of cyber risk disclosure in 10-K. These results show that the marginal cost of providing high-quality CRD dominates the marginal benefits of providing high-quality CRD when peer breaches happen. Therefore, firms strategically use generic language in their CRDs, rendering their CRD less informative.

Table 4.2. The Impact of Peer Breaches on Cyber Risk Disclosure Quality

	(1)	(2)
	CRD	CRD
	Quality	Quality
No. Peer Breaches	-0.010***	-0.014***
	(0.003)	(0.003)
Other Risks Disclosures Length		0.228***
		(0.021)
Has Data Breach This Year		-0.019
		(0.037)
Total Asset		0.047
		(0.029)
Intangible Asset		-0.004
		(0.009)
Operating Expenses		0.068**
		(0.028)
Book Value per Share		0.004
		(0.020)
Employees		-0.004***
		(0.001)
Market HHI		-0.141***
		(0.038)
Internal Weakness		-0.013
		(0.010)
R-squared	0.707	0.710
Observations	19152	18002
No. Firms	4347	4116
Firm and Year FE	YES	YES

Notes: Robust standard errors are in parentheses.

*** p<0.01, ** p<0.05, * p<0.1

4.6 Robustness Analyses

The analyses have two main empirical challenges: omitted variable bias and measurement errors. The omitted variables bias suggests that time-variant industrial shocks might confound the impact of peer breaches, which may bias our results. To mitigate the concern, we perform instrumental variable analyses and incorporate industry and state-specific trends in the model. Similarly, measurement errors may systematically bias our results. Therefore, we use alternative measurements to test if our primary findings are robust.

4.6.1 Main Effect: Instrumental Variables

We first use instrumental variables and perform 2SLS estimations. In our context, the desired instrumental variables should (1) have a relatively strong association with the count of peer breaches and (2) not affect the focal firm's cyber risk disclosure through other channels. Based on those conditions, we use two instrumental variables. They can proxy the complexity of IT infrastructure (i.e., IT complexity) in firms. The main intuition is that peer firms' overall IT complexities are plausibly positively associated with the likelihood of data breaches. However, they do not directly affect a focal firm's CRD quality.

One instrument is the average number of software manufacturers with whom a firm contract (i.e., use their products). Another instrument is the average number of in-house applications present in breached peers' installed IT products. To obtain the measurements, we use the Computer Intelligence Technology Database (CITDB). It is a proprietary dataset commonly used in IT and organization studies (e.g., Forman and van Zeebroeck 2012, Kleis et al. 2012, Cheng et al. 2021). The dataset covers business, operations, and information technology characteristics of more than one million business establishments in the U.S. From the dataset, we can identify the number of software manufacturers and the average number of in-house applications in breached peers each year. Next, we provide a more detailed discussion about these two instruments.

The number of software vendors positively affected the data breach likelihood through two main channels. First, system fragmentation lowers the effectiveness of cybersecurity programs. Software vendors have various design ideologies and maintenance plans, which may cause frictions in applying a unified security program (Newman 2017). For instance, security patch management becomes substantially inefficient when more vendors release patches in an uncoordinated manner (Cavusoglu et al. 2008). Second, a few software vendors may not have the incentive to improve their products' security level. Many vendors choose to release products earlier to gain first-mover advantage (Financial Times 2014, Eastwood 2021). Therefore, a firm that adopts products from more software vendors is more likely to experience security risks.

Furthermore, the number of in-house applications increases a firm's breach risks. First, a firm's internal teams have relatively limited expertise (Ustinov 2021). Since cyber risks evolve fast, it is challenging for the teams to catch up and remediate new threats timely. It is especially the case when in-house applications are used for a long time. Second, maintenance costs of in-house applications are substantially high (Vice 2022). Therefore, firms may underinvest in security protection and expose themselves to higher risks. Consequently, data breaches are more likely to happen in firms that own more in-house applications.

We present our results in Table 4.3. In stage one, the coefficients of instruments are significantly and positively associated with the count of peer breaches, suggesting that peer firms that contract with more IT manufacturers and develop more in-house applications are more likely to experience security breaches. The results are consistent with our theories above. In stage two, the coefficient of the main variable of interest - the number of peer breaches is significantly negative. It supports our main finding in the main models. Furthermore, in the 2SLS analyses, the Kleibergen-Paap rk Wald F statistics is 2315 and Hansen J p-value is 0.532, suggesting that the instruments are not weakly associated with peer breaches and meet the exclusion restriction.

Table 4.3. Instrument Variables - 2SLS Estimations

	(1) Stage 1 Peer Breaches	(2) Stage 2 CRD Quality
No. Software Manufactures (Breached Peers)	1.056*** (0.018)	
No. In-house Apps (Breached Peers)	0.892*** (0.202)	
No. Peer Breaches		-0.019*** (0.005)
Other Risks Disclosures Length	0.021 (0.037)	0.228*** (0.021)
Has Data Breach This Year	0.151 (0.130)	-0.012 (0.036)
Total Asset	-0.056 (0.039)	0.046 (0.029)
Intangible Asset	0.005 (0.014)	-0.004 (0.009)
Operating Expenses	0.179*** (0.036)	0.069** (0.027)
Book Value per Share	0.037 (0.029)	0.004 (0.020)
Employees	-0.002 (0.002)	-0.004*** (0.001)
Market HHI	-0.169*** (0.041)	-0.144*** (0.037)
Internal Weakness	0.010 (0.012)	-0.013 (0.010)
R-squared		0.045
Observations	17371	17371
No. Firms	3486	3486
Kleibergen-Paap rk LM statistic		2315
Hansen J p-value		.532
Firm and Year FE		YES

Notes: Robust standard errors are in parentheses. *No. Software Manufactures (Breached Peers)* is the average of the number of software manufactures that breached peers contract with. *No. In-house Apps (Breached Peers)* is the average of the number of adopted in-house apps in breached peers.

*** p<0.01, ** p<0.05, * p<0.1

4.6.2 Main Effect: Industry and State Specific Trends

Industrial-level events, such as technology innovations, business or operations standards implementations, or demand shocks, may change firms' strategies and disclosure. Similarly, peer firms located in the same states may be affected by the enforcement of privacy and security regulations simultaneously, leading to shifts in their disclosure incentives. Therefore, those major events may confound our results. To address the issue, we incorporate industry- and state-year fixed effects in the analyses. Note that we denote firms with two-digit SIC codes as they are in the same industry following previous practices (Kamiya et al. 2021, Gordon et al. 2010). Next, we incorporate *Industry Indicator* \times *Year* and *States Indicator* \times *Year* separately in the regression. Although the fixed effects absorb substantial variations, the results in Columns (1) and (2) of Table 4.4 remain consistent with our main findings.

4.6.3 Main Effect: Alternative Measurements

Measurement choices may substantially affect the results. In particular, the main outcome variable in our analyses is a constructed variable based on textual features. To mitigate the concern that the main finding is sensitive to different choices, we use an alternative measurement of the outcome variable. Instead of using the corpus based on yearly disclosure documents, we leverage the corpus based on disclosure documents from 2011 to 2017 and construct an alternative outcome variable. In addition, we use an alternative binary treatment variable *Peer Breach Indicator* to denote if a firm has more than one peer experience data breaches.³ Next, we perform the regression analyses using the alternative outcome and treatment variables and report results in Table 4.5. Results in Column (1) and Column (2) show that the coefficient of *No. Peer Breaches* and *Peer Breach Indicator* are significantly positive, suggesting that our main findings are robust to the alternative measurements.

³In our sample, the fourth quartile of peer breaches is 2.

Table 4.4. Industry and State Specific Trends

	(1) Industry-Year FE	(2) State-Year FE
No. Peer Breaches	-0.010** (0.005)	-0.015*** (0.003)
Other Risks Disclosures Length	0.229*** (0.021)	0.238*** (0.023)
Has Data Breach This Year	-0.019 (0.035)	-0.016 (0.038)
Total Asset	0.094*** (0.029)	0.029 (0.030)
Intangible Asset	0.000 (0.009)	0.001 (0.010)
Operating Expenses	0.041 (0.028)	0.087*** (0.028)
Book Value per Share	0.015 (0.020)	0.008 (0.021)
Employees	-0.003*** (0.001)	-0.004*** (0.001)
Market HHI	-0.125*** (0.037)	-0.144*** (0.038)
Internal Weakness	-0.012 (0.009)	-0.017* (0.010)
Constant	-1.289*** (0.218)	-1.132*** (0.235)
R-squared	0.721	0.702
Observations	17345	16573
No. Firms	3867	3659
Firm and Year FE	YES	YES

Notes: Robust standard errors are in parentheses

*** p<0.01, ** p<0.05, * p<0.1

Table 4.5. Alternative Measurements

	(1) CRD Quality Based on All Corpus	(2) Binary Treatment
No. Peer Breaches	-0.015*** (0.003)	
Peer Breach Indicator		-0.031* (0.017)
Other Risks Disclosures Length	0.206*** (0.018)	0.227*** (0.021)
Has Data Breach This Year	-0.049 (0.041)	-0.030 (0.036)
Total Asset	-0.008 (0.030)	0.048* (0.029)
Intangible Asset	-0.004 (0.010)	-0.004 (0.009)
Operating Expenses	0.081*** (0.028)	0.065** (0.027)
Book Value per Share	0.013 (0.022)	0.004 (0.020)
Employees	-0.004*** (0.001)	-0.004*** (0.001)
Market HHI	-0.135*** (0.039)	-0.135*** (0.037)
Internal Weakness	-0.004 (0.010)	-0.013 (0.010)
Constant	-0.635*** (0.211)	-1.039*** (0.217)
R-squared	0.682	0.697
Observations	17371	17371
No. Firms	3492	3492
Firm and Year FE	YES	YES

Notes: Robust standard errors are in parentheses

*** p<0.01, ** p<0.05, * p<0.1

4.7 Heterogeneity Analyses

In this section, we analyze the mechanisms underlying the main effect. To do so, we investigate two main channels through which peer breaches discourage CRD. These two channels are (1) peer breaches induce a higher expected likelihood that CRD may cause cyber risks, and (2) peer breaches exacerbate the negative market reactions to CRD.

4.7.1 Internal Risks Assessment

Peer breaches raise the expected cost of CRD by increasing the likelihood of cyber risks. As a result, managers of the focal firm strategically lower the CRD quality. If so, this effect of peer breaches would be enhanced when the firm is inherently more susceptible to data breaches. We utilize two proxies to measure how vulnerable a firm is to breach incidents. These two proxies are (1) the number of sites and (2) the value of intangible assets.

A firm with more sites is more likely to experience data breaches. First, having more sites implies that a firm's IT infrastructure is more complex, and its attacking surface is larger (Tanriverdi et al. 2019). Therefore, increasing endpoints and inter-linkages produce exploitable vulnerabilities, making it easier for hackers to attack. Second, it is becoming more challenging to implement IT security control in many business units (Liu et al. 2020). Besides, IT security control is less effective when business sites are dispersed (Pang and Tanriverdi 2022). Business operations in different sites involve a higher number of employees and contractors. Hence, the human factors may weaken protection and cause internal breaches. If a firm owns a larger size of intangible assets, its data breach likelihood could also be higher. First, the size of intangible assets is positively associated with intruders' benefits from attacking the firm. According to the rational choice theory (Becker 1968), intruders are more likely to target those whose attack can produce more benefits. Therefore, a firm with more intangible assets is more susceptible to data breaches. Second, firms with intangible

assets usually have a higher reputation. The high visibility may also attract intruders to conduct attacks.

To examine the mechanism, we first obtain the *No. Sites* from CITDB and *Intangible Assets* from COMPUSTAT. Next, we incorporate the interaction term *No. Peer Breaches* \times *No. Sites* and *No. Peer Breaches* \times *Intangible Assets* in the model specifications, respectively. Table 4.6 presents our findings. Column (1) shows that the coefficient of *No. Peer Breaches* \times *No. Sites* is significantly negative, suggesting that the negative effect of peer breaches on CRD quality is higher on firms having more sites. Column (2) presents that the coefficient of *No. Peer Breaches* \times *Intangible Assets* is significantly negative, suggesting that the negative effect of peer breaches on CRD quality is enhanced if a firm has a larger size of intangible assets. Consistent with our reasoning, litigation concerns are more significant if firms are more susceptible to data breach risks.

Table 4.6. Heterogeneity Analysis: Susceptibility to Data Breaches Risks

	(1) CRD Quality	(2) CRD Quality
No. Peer Breaches	0.021** (0.008)	
No. Peer Breaches \times No. Sites	-0.010*** (0.002)	
No. Peer Breaches \times Intangible Asset		-0.004*** (0.001)
No. Sites	-0.009 (0.011)	
Intangible Asset	0.004 (0.011)	-0.001 (0.009)
R-squared	0.669	0.698
Observations	11027	17371
No. Firms	2072	3492
Firm and Year FE	YES	YES

Notes: Robust standard errors are in parentheses. We use the log of the number of sites and the log of the intangible asset values. All relevant control variables are included. *** $p < 0.01$, ** $p < 0.05$, * $p < 0.1$

4.7.2 Public Attention

Peers' breaches can have negative spillover effects because investors may think similar firms are exposed to similar cyber risks. Consequently, a firm's cost of disclosing cyber risks becomes higher when its peer experience breaches. It is especially the case when the public pays substantial attention to data security. Therefore, we use several proxies to measure the strength of public attention, including (1) internet search trends, (2) focal firms' advertising expenditure, and (3) if the focal firms are in service-related industries.

A high level of public attention suggests that the severity of incidents or the stringency of regulations are well-recognized by the public during a period of time. Therefore, we use internet search on "data breach" to capture the level of public attention. Besides, considering that breaches involving consumer data are usually high-profile, we argue that the strength of public attention is positively associated with the firms' reliance on the consumer market. Furthermore, businesses that rely more on customer trust are more likely to be affected by the negative information spillover effect. Those businesses usually store and leverage a large amount of customer data. In addition, the enforcement of several privacy regulations enhances the awareness of customer data protections. As a result, firms that incur higher advertising expenditure or provide services may experience a larger magnitude of the impact.

We first measure the public attention to data breaches by using Google Trends. Its API allows us to download and aggregate monthly search indices for the keyword "data breaches" from 2011 to 2017. The indices are based on a large number of searches on Google, so they can represent the trend of public interest in a specific topic. Figure 4.8 plots the trend of "data breaches" searches that are used in our analyses. Furthermore, we use *Advertising Expenditure* from COMPUSTAT. Lastly, we construct *Service* indicator using two-digit SIC codes. Specifically, we denote a firm as providing service if its two-digit SIC code is in the ranges from 52-59 (Retail Trade), 69-67 (Finance, Insurance, Real Estate), and 70-89 (Services).

To analyze how the impact of peer breaches varies with public attention, we incorporate $No. Peer Breaches \times Public Attention$, $No. Peer Breaches \times Advertising Expense$, and $No. Peer Breaches \times Service Industry$ in the model specification. Table 4.7 presents our findings. Consistent with our reasoning, the coefficient of all three interaction terms is significantly negative. Therefore, firms tend to substantially decrease CRD quality in response to peer breaches if the level of public attention on data breaches is higher.

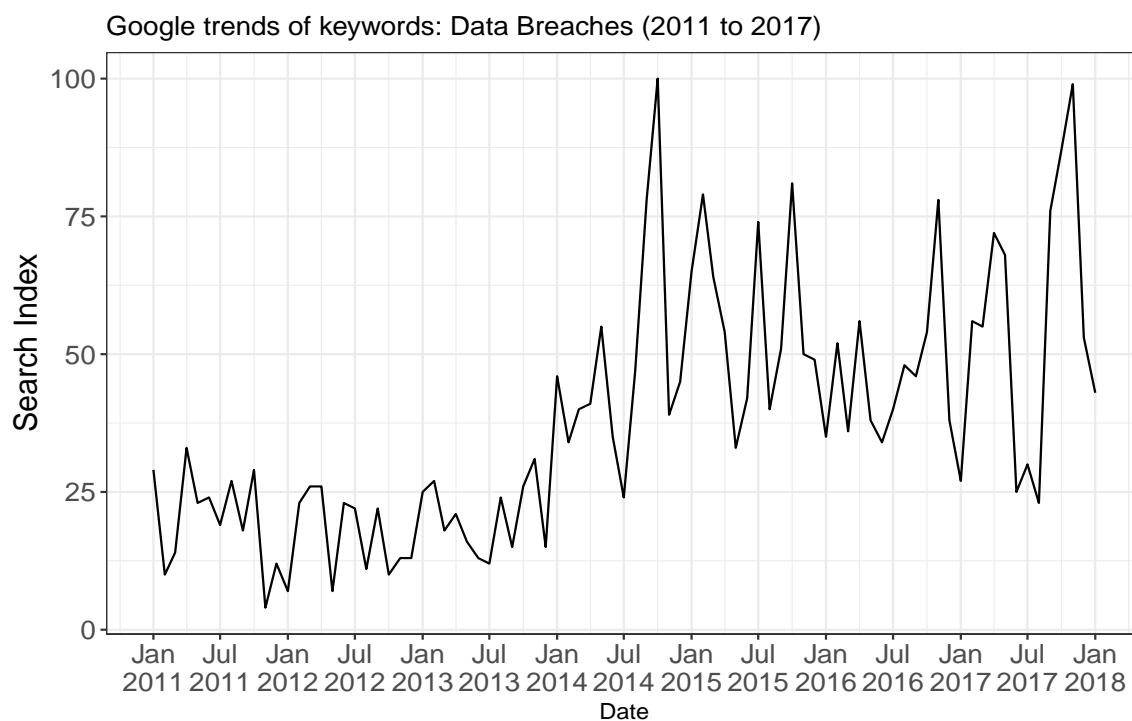


Figure 4.8. Google Trends - Data Breaches

Table 4.7. Heterogeneity Analysis: Public Attention

	(1) CRD Quality	(2) CRD Quality	(3) CRD Quality
No. Peer Breaches	0.071*** (0.008)		-0.011** (0.003)
No. Peer Breaches \times Public Attention	-0.002*** (0.000)		
No. Peer Breaches \times Advertising Expense		-0.008*** (0.001)	
No. Peer Breaches \times Service Industry			-0.014* (0.006)
R-squared	0.701	0.715	0.698
Observations	17371	7647	17371
No. Firms	3492	1624	3492
Firm and Year FE	YES	YES	YES

Notes: Robust standard errors are in parentheses. We use the log of the advertising expenditure. A firm is in the service industry if its two-digit SIC code is in the ranges from 52-59 (Retail Trade), 69-67 (Finance, Insurance, Real Estate), and 70-89 (Services). All relevant control variables are included. *** $p < 0.01$, ** $p < 0.05$, * $p < 0.1$

4.8 Additional Analyses

4.8.1 Cyber Risks Disclosure Length

Firms tend to provide longer and boilerplate disclosure, which are less likely to be deemed inadequate during judicial and regulatory examination (Cazier et al. 2021). Since peer breaches increase the litigation costs, firms may tend to provide longer CRD. In this section, we investigate if firms do so in response to peer breaches.

In the analyses, we use the length of CRD (i.e., the count of words in CRD) as outcome variables. In Column (1) of Table 4.8, the coefficient of peer breaches is significantly positive. All else being equal, one additional peer breach leads to a 0.8% increase in the number of words in cyber risk disclosures. Given that CRD quality decreases, the result provides suggestive evidence that managers want to lower litigation costs by providing longer but less informative CRD in response to peer breaches.

4.8.2 Cybersecurity Investment

A lack of cybersecurity investment is one main driving force of high-security risks among many firms (Anderson and Moore 2006). In other words, firms that substantially adopt security countermeasures and implement IT security policy are less likely to experience breaches (Kwon and Johnson 2014). However, if cybersecurity investment can offset a proportion of inflated expected risks induced by peer breaches is unknown to all. If that is the case, firms that invest in cybersecurity are less likely to lower CRD quality in response to peer breaches. Next, we empirically test the argument.

We use the number of adopted cybersecurity applications (unique number) to proxy a firm’s cybersecurity investment (Angst et al. 2017). The data is from a proprietary dataset - CiTDB. Table C.3 in the Appendix shows all categories of cybersecurity applications captured in the dataset. We incorporate the interaction term $No. Peer Breaches \times Installed Cybersecurity Apps$ in the model specifications. Table 4.8 presents our findings. Column (2) shows that the coefficient of $No. Peer Breaches \times Installed Cybersecurity Apps$ is significantly positive. Interestingly, firms that invest more in cybersecurity are less likely to lower CRD quality when peers experience breaches. In other words, a firm with a good security posture may leverage the peer breaches to disclose more specific and detailed cyber risks and risk management strategies. We speculate that those firms may want to increase visibility and reputation by providing high-quality CRD and differentiating themselves from breached peers.

4.8.3 Analyst Coverage

In capital markets, analysts are professionals who study specific firms and track their information, and then publish reports and make recommendations about firms’ securities. They play a vital role in acquiring and analyzing data pertinent to a firm’s assessment. As experts in specific industries, analysts can act as “information bridges” to translate firms’ signals into insights that could be helpful for investors

(Havakhor et al. 2020, Barber et al. 2001). As major events, data breaches are likely to be captured by analysts. As a result, cybersecurity might be a factor they consider in providing investment suggestions. If analysts are perceived as capable of understanding and questioning firms' cybersecurity strategies, the analyst coverage presumably mitigates the negative impact of peer breaches.

To analyze the impact of analyst coverage, we obtain data on the number of analysts who cover certain firms from IBES. Next, we incorporate the interaction term *No. Peer Breaches* \times *Analyst Coverage* in the model specifications. Column (3) of Table 4.8 presents the findings consistent with our reasoning. The magnitude of quality reduction induced by peer breaches moderately decreases when firms have more analyst coverage.

Table 4.8. Additional Analyses

	(1)	(2)	(3)
	Outcome: CRD Length	Cybersecurity Investment	Coverage
No. Peer Breaches	0.882** (0.417)	-0.030*** (0.005)	-0.023*** (0.006)
No. Peer Breaches \times Installed Cybersecurity Apps		0.043*** (0.009)	
No. Peer Breaches \times Analyst Coverage			0.002* (0.001)
R-squared	0.802	0.644	0.679
Observations	17371	8896	6522
No. Firms	3492	1640	1425

Notes: Robust standard errors are in parentheses. We use the log of the word count as CRD Length. All relevant control variables are included.

*** $p < 0.01$, ** $p < 0.05$, * $p < 0.1$

4.9 Summary and Discussion

4.9.1 Conclusion and Contribution

This study investigates how peer breaches affect firms' voluntary disclosure of cyber risks. Although firms provide lengthier discussions on cyber risks after peer breaches, our results suggest that the quality of the cyber risk disclosure significantly decreases. Furthermore, we explore two mechanisms - internal litigation concerns and external market perceptions. Our findings demonstrate that the negative impacts are enhanced on firms with more sites or owning a larger size of intangible assets. Besides, peer breaches exert a larger effect when the public attention to data breaches is high, when the focal firm substantially invests in advertising, or when the focal firm is in the service industry. The findings uncover the unintended consequences of data breaches which impairs the information environment by discouraging informativeness CRD from a group of peer firms. In addition, firms provide longer CRD in response to peer breaches. Lastly, the decrease in disclosure quality can be mitigated if a firm invests more in cybersecurity or has more analysts covering it.

This study makes several theoretical contributions. First, it complements the information security literature by examining how firms react to peer breaches. Furthermore, the study contributes to the accounting literature by discussing corporations' incentives in disclosing cyber risks. Third, we discuss potential mechanisms that shed light on how managers make decisions in disclosures depending on their firms' cyber risks and the public's attention to data breaches. In addition, the study offers some practical implications. It uncovers the unintended consequences of data breach incidents. Policymakers need to consider the cost when allocating resources to deter cyber incidents. Furthermore, SEC needs to design better incentives to encourage firms to provide informative cyber risk disclosures.

4.9.2 Limitations and Future Directions

The study has several limitations. First, our study does not analyze the financial outcomes that may be affected by peer breaches as an information event. Future research can further investigate if peer breaches degrade the information environment to derive the economic magnitude of the impact. To do so, researchers must rigorously examine how data breaches affect several key financial indicators, such as stock price volatility and information efficiency.⁴

Second, we focus on textual informativeness (i.e., textual similarity) of CRD as an outcome. Future research can further explore different measurements of quality and other textual features that may be affected by peer breaches. Those features may include topics, tone, and sentiments, among others.

Third, endogeneity is a concern in our research, as it is in many observational studies. The whole causation cannot be proven using secondary data such as ours, although we properly address these problems using identification procedures to mitigate concerns regarding omitted variables and measurement errors.

Lastly, policies regarding CRD have been evolving, which may change CRD dynamics. In 2022, the SEC proposed rules on enhancing cyber risks disclosures (SEC 2022). Future studies can analyze the CRD in the post-policy financial filings to test if our findings hold.

Our study's limitations provide opportunities for future research. We believe that the study of corporate strategies in managing cyber risks is likely to be a fruitful area for future research.

⁴Information efficiency can be measured as the difference between the cumulative abnormal returns before and after an information event. A larger (smaller) gap implies less information efficiency (Francis et al. 2006).

CHAPTER 5

SUMMARY AND FUTURE RESEARCH

The importance of information security will be continuously increasing along with the growing reliance on cutting-edge technologies such as business analytics, cloud solutions, and artificial intelligence. Research from management perspectives is valuable to illuminate practical questions that organizations or individuals confront in securing their digital assets. Building on literature and theories from Information Systems (IS) and economics, my dissertation investigates a few relevant questions and hopefully contributes to this area.

The first essay investigates how sharing electronic health data via Health Information Exchanges (HIEs) affects hospitals' data breach risks. It contributes to three streams of literature in the IS field. First, it extends the information security literature in the inter-organizational system context. This study is the first to investigate changes in realized security risks after hospitals start to share data electronically across organizational boundaries. Second, it contributes to the inter-organizational system (IOS) literature. Our findings illustrate the unexpected effects of breaking information silos among organizations' coordination in the information security field. Third, this study complements the health IT literature. Our findings provide evidence that governance in HIEs may facilitate coordination in the cybersecurity landscape, thereby improving the overall security performance in hospitals. Furthermore, it suggests that HIE is more than providing a channel for hospitals to exchange medical information and knowledge. The governance in the process is critical in mitigating risks, which is worthy of further investigation. Furthermore, different stakeholders need to realize how connecting to HIEs impacts hospitals' security postures, given the increasing prominence of privacy and security in data sharing.

The second essay examines a bug bounty program's incentive design and cost-effectiveness using game-theoretical models. It makes several contributions. First, it examines the role of organization security features, participating security researchers, and legal regimes in BBPs. Therefore, it provides a framework for designing an organization's crowdsourcing cybersecurity solution. Second, our model treats BBP as a layer in organization vulnerability management in which an organization's own security capability can affect the payoffs of the program. Third, it complements tournament literature by discussing how security researchers' productivity heterogeneity and their total number affect dynamics in the specific security context. Lastly, the study reveals that legal protection for security researchers may benefit organizations. Those findings offer managerial insights for security practitioners, organizations, and policy makers in designing BBP as a crowdsourcing cybersecurity solution.

The third essay investigates how peer breaches affect firms' voluntary disclosure of cyber risks. This study makes several theoretical contributions. First, it complements the information security literature by examining how firms react to peer breaches. Furthermore, the study contributes to the accounting literature by discussing corporations' incentives in disclosing cyber risks. Third, we discuss potential mechanisms that shed light on how managers make decisions in disclosures depending on their firms' cyber risks and the public's attention to data breaches. In addition, the study offers some practical implications. It uncovers the unintended consequences of data breach incidents. Policymakers need to consider the cost when allocating resources to deter cyber incidents. Furthermore, SEC needs to refine guidance to encourage firms to provide informative cyber risk disclosures.

Overall, the dissertation offers some unique and new perspectives on information security management. In particular, it emphasizes *coordination* in controlling IT risks and protecting digital assets. First, its three essays present different types of coordination mechanisms in dealing with cybersecurity. The first two essays focus on the benefits of connecting peer hospitals and involving external groups. The last essay explores the unintended spillover effect among peer firms. Second, it investigates heterogeneities and limitations that should be considered when designing or

applying those mechanisms. Lastly, it provides theories that can be generalized to other scenarios that require coordination. The dissertation can serve as a starting point for further discussion and encourage more in-depth research on similar topics.

APPENDICES

A APPENDIX - STUDY 1

Table A.1. Correlation Matrix

Variables	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)	(13)
(1) Data Breach	1.00												
(2) IT System Breach	0.66	1.00											
(3) Physical Breach	0.58	0.00	1.00										
(4) Hacker Attacking	0.54	0.74	0.04	1.00									
(5) Insider Breach	0.34	0.25	0.11	-0.01	1.00								
(6) Unintended Disclosure	0.61	0.22	0.36	-0.01	0.01	1.00							
(7) Join HIE	0.01	0.01	0.02	-0.02	-0.00	0.02	1.00						
(8) IT Security Capability	0.01	-0.01	0.00	-0.01	0.00	0.03	-0.06	1.00					
(9) HIE Security Laws	-0.01	0.01	0.01	-0.00	-0.02	-0.01	0.10	0.04	1.00				
(10) Health System Size	0.14	0.14	0.02	0.14	0.03	0.06	0.03	0.10	-0.04	1.00			
(11) Operation Expenditure	0.15	0.06	0.12	0.03	0.07	0.11	0.13	0.15	-0.07	0.26	1.00		
(12) IT apps	0.09	0.04	0.04	0.01	0.06	0.07	0.27	0.24	0.02	0.18	0.59	1.00	
(13) Admin Apps	0.08	0.04	0.02	0.01	0.05	0.07	0.23	0.25	0.01	0.18	0.39	0.84	1.00
(14) Strategy Apps	0.03	0.03	0.02	-0.00	0.04	0.00	0.24	0.20	0.01	0.23	0.37	0.81	0.74
(15) Clinic Apps	0.10	0.04	0.05	0.00	0.05	0.09	0.24	0.14	0.01	0.05	0.63	0.90	0.66
(16) MU1	0.08	0.05	-0.01	0.07	0.04	0.05	0.01	-0.02	0.04	-0.07	0.08	0.20	0.17
(17) IS Plan	-0.04	-0.07	-0.02	-0.12	0.01	0.03	0.14	0.21	0.02	0.29	0.15	0.26	0.23
(18) MSA	0.07	0.01	0.06	0.00	0.03	0.07	0.08	0.17	-0.05	0.41	0.51	0.26	0.22
(19) Academic	0.07	0.01	0.10	0.01	0.03	0.04	0.05	0.02	-0.02	0.03	0.31	0.14	0.11
(20) For Profit	-0.01	0.08	-0.05	0.12	-0.04	-0.07	-0.12	-0.01	-0.02	0.51	-0.19	-0.25	-0.16
(21) Competition	-0.04	0.01	-0.03	0.02	-0.01	-0.04	-0.03	-0.02	0.02	-0.11	-0.13	-0.07	-0.05
(22) CMI	0.03	-0.03	0.04	-0.03	0.01	0.04	0.11	0.07	0.14	0.08	0.19	0.13	0.09
(23) Income	0.05	0.01	0.03	-0.00	0.01	0.06	0.14	0.09	0.10	0.16	0.26	0.14	0.12
(24) Population	0.10	0.02	0.08	-0.01	0.03	0.11	0.07	0.17	-0.04	0.45	0.54	0.26	0.24
(25) Unemployment	-0.00	-0.04	0.02	-0.03	-0.00	0.01	-0.26	0.01	-0.31	0.05	0.12	-0.05	-0.04
Variables	(14)	(15)	(16)	(17)	(18)	(19)	(20)	(21)	(22)	(23)	(24)	(25)	
Strategy Apps	1.00												
(15) Clinic Apps	0.62	1.00											
(16) MU1	0.14	0.23	1.00										
(17) IS Plan	0.29	0.16	-0.10	1.00									
(18) MSA	0.23	0.18	-0.07	0.22	1.00								
(19) Academic	0.11	0.14	0.02	0.00	0.12	1.00							
(20) For Profit	-0.08	-0.36	-0.13	0.03	0.18	-0.08	1.00						
(21) Competition	-0.06	-0.05	0.04	-0.05	-0.15	-0.06	-0.09	1.00					
(22) HRR CMI	0.11	0.10	0.01	0.14	0.23	0.06	-0.03	-0.12	1.00				
(23) Income	0.13	0.10	0.01	0.14	0.33	0.13	0.01	-0.21	0.31	1.00			
(24) Population	0.25	0.18	-0.08	0.25	0.77	0.16	0.23	-0.37	0.31	0.42	1.00		
(25) Unemployment	-0.08	-0.03	-0.04	-0.06	0.07	0.01	0.04	-0.03	-0.16	-0.47	0.15	1.00	

Table A.2. Robustness Check: State-year Specific Trends

DV: Data Breach	(1)	(2)	(3)
Join HIE	-0.016*	0.029+	-0.009
	(0.007)	(0.016)	(0.009)
Join HIE* IT Security Capability		-0.012**	
		(0.004)	
Join HIE*HIE Security Laws			-0.022+
			(0.013)
R-squared	0.344	0.352	0.344
Observations	9373	9161	9373
No. Hospitals	1642	1635	1642
Hospital & Year FE & Control Variables	YES	YES	YES
State-year specific trends	YES	YES	YES

Notes: All estimations use cluster-adjusted robust standard errors (clustered at the hospital level).

*** p<0.001, ** p<0.01, * p<0.05, +p<0.1

Table A.3. Robustness Check: Non-linear Models

DV: Data Breach	(1)	(2)	(3)
	Probit models		
Join HIE	-0.199*	0.520*	-0.045
	(0.092)	(0.224)	(0.106)
Join HIE* IT Security Capability		-0.170**	
		(0.056)	
Join HIE*HIE Security Laws			-0.425*
			(0.169)
Log-likelihood	-1250.658	-1237.999	-1259.830
Observations	9407	9203	9407
No. Hospitals	1601	1601	1601
Year FE &Control Variables	YES	YES	YES

Notes: Since we use Probit models, hospitals fixed effects cannot be implemented. To mitigate the endogeneity concern, we add time-invariant covariates (i.e., Academic, MSA location, For-Profit) in model specifications and use matched sample. All estimations use robust standard errors. *** p<0.001, ** p<0.01, * p<0.05, +p<0.1

B APPENDIX - STUDY 2

B.1 Main Model

Proofs of Lemma 3.3.1, Lemma 3.3.2, and Corollary 3.3.1

First, we discuss Lemma 3.3.1. For each security researcher i , the objective function is $blP(g_i > g_{-i}) - ce$. Performance v can be written as a function of security researcher's productivity, which is $g_i = r(a_i e_i)$. Therefore, the objective function equals to $blP(g(a_i) > g_{-i}) - cr^{-1}(g)/a_i$. Since the distribution of productivity is Q , $P(g(a_i) > g_{-i})$ equals to $Q(g_{-i}^{-1}(g_{-i}))$ where g_{-i} represents others' strategies. Furthermore, we consider a symmetric Bayesian game, every security researcher in the game use the same strategy. Then we take derivative of the objective function and obtain the first-order condition $\frac{b(Q_1^{n-1}(a_i))'}{(a_i e'(a_i) + e(a_i))r'(a_i e(a_i))} - \frac{c}{a_i r'(a_i e(a_i))} = 0$. Next, we take integral of the first-order condition and obtain the equilibrium effort: $e_i^* = \frac{b \int_{\underline{a}}^{a_i} a q_1^{n-1}(a) da}{c a_i}$ where $(Q_1^{n-1}(a))' = q_1^{n-1}(a)$. Since $Q \sim U[\underline{a}, \bar{a}]$, we can write the optimal effort as $\frac{bl \left(\frac{a_i - \underline{a}}{\bar{a} - \underline{a}} \right)^{n-1} (\underline{a} + (n-1)a_i)}{c n a_i}$.

Second, we analyze Lemma 3.3.2. Given the optimal level of effort of security researcher, individual performance g_i^* equals to $\frac{bl \left(\frac{a_i - \underline{a}}{\bar{a} - \underline{a}} \right)^{n-1} (\underline{a} + (n-1)a_i)}{cn}$ since we use a linear performance function $v = a * e$. Then the best performance among security researchers is $\int_{\underline{a}}^{\bar{a}} g_i q_1^n(a_i) da_i$. We plug $q_1^n(a_i)$ and g_i , obtaining the best performance as $\frac{bl((n-1)(2n-1)\bar{a} + \underline{a}(3n-1))}{2cn(2n-1)}$. Since the performance of security researchers is negatively associated with earliest discovery time of a vulnerability, we use a linear function and obtain the expected earliest discovery time $\mathbb{E}[I] = T - \frac{bl((n-1)(2n-1)\bar{a} + \underline{a}(3n-1))}{2cn(2n-1)}$. Taking the expressions into account, the total cost for the organization can be written as:

$$\Pi = \beta c_a (1 - b\theta) \left(\frac{bl(((3-2n)n-1)\bar{a} - 3\underline{a}n + \underline{a})}{2cn(2n-1)} + \beta\omega + T \right) + \beta bl n \omega c_p + b. \quad (1)$$

The first order condition along with the non-negative nature of the bounty reveal that

$$b^* = \frac{1}{2\theta} - \frac{2cn(2n-1)(-\beta\theta c_a(\beta\omega + T) + \beta ln \omega c_p + 1)}{2\theta \beta l c_a ((n-1)(2n-1)\bar{a} + (3n-1)\underline{a})}. \quad (2)$$

The second order condition $\frac{\beta\theta l c_a((n-1)(2n-1)\bar{a}+\underline{a}(3n-1))}{cn(2n-1)}$ (positive) implies that b^* is the equilibrium bounty in the BBP. The equilibrium values of the expected earliest discovery time and total post-discovery cost in Corollary 3.3.1 are derived by substituting the solution for the optimal bounty (i.e., b^*) to expected damage cost (i.e., $\mathbb{E}[I^*] = T - \frac{b^*l((n-1)(2n-1)\bar{a}+\underline{a}(3n-1))}{2cn(2n-1)}$) and post-discovery cost (i.e., $K^* = b^*l\omega\beta$) respectively. ■

Proofs of Proposition 3.4.1

First, we analyze part (i) of Proposition 3.4.1. We take derivative of the optimal bounty (2) with respect to the patching complexity ω and obtain $\frac{db^*}{d\omega} = \frac{cn(2n-1)(\beta\theta c_a - lnc_p)}{\theta l c_a((n-1)(2n-1)\bar{a}+(3n-1)\underline{a})}$. Upon examination of the derivative, we can write the threshold value for β as $\frac{lnc_p}{\theta c_a}$. If β is below the threshold, the optimal bounty decreases in the patching complexity. Otherwise, the optimal bounty increases in the patching complexity.

Next, we discuss part (ii) of Proposition 3.4.1. Derivative of the optimal bounty (2) with respect to the security posture is given by $\frac{db^*}{d\beta} = \frac{cn(2n-1)(\beta^2\theta\omega c_a + 1)}{\beta^2\theta l c_a((n-1)(2n-1)\bar{a}+(3n-1)\underline{a})}$. Given all constraints, the derivative is always positive, suggesting that the optimal bounty always increase an organization's security posture. Hence the proof. ■

Proofs of Proposition 3.4.2

We first discuss part (i) of Proposition 3.4.2. Derivative of the equilibrium bounty with respect to the higher bound (i.e., \bar{a}) and lower bound (i.e., \underline{a}) of the efficiency is given as

$$\frac{db^*}{d\bar{a}} = \frac{cn(n(6n-5)+1)(-\beta\theta c_a(\beta\omega+T) + \beta l n \omega c_p + 1)}{\beta\theta l c_a((n-1)(2n-1)\bar{a} + \underline{a}(3n-1))^2}, \quad (3)$$

$$\frac{db^*}{d\underline{a}} = \frac{c(1-2n)^2(n-1)n(-\beta\theta c_a(\beta\omega+T) + \beta l n \omega c_p + 1)}{\beta\theta l c_a((n-1)(2n-1)\bar{a} + \underline{a}(3n-1))^2}. \quad (4)$$

Hence, both of (3) and (4) are positive if and only if $-\beta\theta c_a(\beta\omega+T) + \beta l n \omega c_p + 1 > 0$. Upon examination of the derivative, we can write the threshold value for θ as $\frac{\beta l n \omega c_p + 1}{\beta c_a(\beta\omega+T)}$. If θ is below the threshold, $-\beta\theta c_a(\beta\omega+T) + \beta l n \omega c_p + 1 > 0$, the bounty

increases in the security researchers' efficiencies. Otherwise, the organization lowers the bounty when security researchers have higher efficiencies.

Let us now discuss part (ii) of the proposition. We define $A_1 = (3(3-4n)n-2)$ and $A_2 = (1-2n)^2\bar{a}(\beta\theta c_a(\beta\omega+T) + \beta l(n-2)n\omega c_p - 1)$. Derivative of the equilibrium bounty (2) with respect to the number of security researcher n is given as:

$$\frac{db^*}{dn} = \frac{c(\underline{a}(\beta^2\theta(6n^2-4n+1)\omega c_a + \beta\theta(6n^2-4n+1)Tc_a + \beta lnA_1\omega c_p - 6n^2 + 4n - 1) - A_2)}{\beta\theta l c_a((n-1)(2n-1)\bar{a} + (3n-1)\underline{a})^2}. \quad (5)$$

Upon examination of the derivative (5), the denominator is always positive. Based on the numerator, we can write the threshold value for θ as

$$\hat{\theta}_1 = \frac{\underline{a}(n(\beta l A_1 \omega c_p - 6n + 4) - 1) - (1 - 2n)^2 \bar{a}(\beta l(n - 2)n\omega c_p - 1)}{\beta c_a(\beta\omega + T)((1 - 2n)^2 \bar{a} + \underline{a}(-6n^2 + 4n - 1))}.$$

Next, we analyze how the relationship between θ and $\hat{\theta}_1$ affects the sign of (5). Derivative of the numerator of (5) with respect to θ is

$$-c\underline{a}(\beta^2(6n^2-4n+1)\omega c_a + \beta(6n^2-4n+1)Tc_a) - \beta(1-2n)^2\bar{a}c_a(\beta\omega+T)$$

which can be written as $-\beta c_a((-6n^2+4n-1)\underline{a} + (1-2n)^2\bar{a})(\beta\omega+T)$. Considering all constraints, we find that the sign of $(-6n^2+4n-1)\underline{a} + (1-2n)^2\bar{a}$ can determine the direction of how θ affect $\frac{db^*}{dn}$. Specifically, when $(-6n^2+4n-1)\underline{a} + (1-2n)^2\bar{a} < 0$ ($\frac{\bar{a}}{\underline{a}} \leq \frac{6n^2-4n+1}{(1-2n)^2}$), $\frac{db^*}{dn}$ increases in θ . As a result, $\frac{db^*}{dn} > 0$ if and only if $\theta > \hat{\theta}_1$. However, if $(-6n^2+4n-1)\underline{a} + (1-2n)^2\bar{a} > 0$ ($\frac{\bar{a}}{\underline{a}} > \frac{6n^2-4n+1}{(1-2n)^2}$), $\frac{db^*}{dn}$ decreases in θ . This means $\frac{db^*}{dn} > 0$ if and only if $\theta < \hat{\theta}_1$. ■

Proofs of Proposition 3.4.3

To get the equilibrium total cost, we first plug the optimal bounty (2) into the objective function (1). Thus, the equilibrium total cost can be written as

$$\Pi^* = \frac{\frac{\beta l c_a((3-2n)n-1)\bar{a}-3n\underline{a}+\underline{a}}{cn(2n-1)} - \frac{4cn(2n-1)(-\beta\theta c_a(\beta\omega+T)+\beta ln\omega c_p+1)^2}{\beta l c_a((n-1)(2n-1)\bar{a}+(3n-1)\underline{a})} + 4\beta(\theta c_a(\beta\omega+T) + ln\omega c_p) + 4}{8\theta} \quad (6)$$

Next, we discuss part (i) of Proposition 3.4.3. We take the derivative of the equilibrium total cost with respect to \underline{a} and \bar{a} , obtaining

$$\frac{d\Pi^*}{d\underline{a}} = \frac{\frac{4cn(n(6n-5)+1)(-\beta\theta c_a(\beta\omega+T)+\beta l n\omega c_p+1)^2}{\beta l c_a((n-1)(2n-1)\bar{a}+(3n-1)\underline{a})^2} + \frac{\beta l(1-3n)c_a}{cn(2n-1)}}{8\theta}, \quad (7)$$

$$\frac{d\Pi^*}{d\bar{a}} = \frac{\frac{4c(1-2n)^2(n-1)n(-\beta\theta c_a(\beta\omega+T)+\beta l n\omega c_p+1)^2}{\beta l c_a((n-1)(2n-1)\bar{a}+(3n-1)\underline{a})^2} - \frac{\beta l(n-1)c_a}{cn}}{8\theta}. \quad (8)$$

Both of (7) and (8) are always negative given our constraints. The results suggest that if security researchers (novices and experts) become more efficient, the total cost strictly decreases. The differences between the two marginal effects can be written as $\frac{d\Pi^*}{d\underline{a}} - \frac{d\Pi^*}{d\bar{a}} = \frac{((n-3)n+1)\left(\beta^2 l^2 c_a^2 - \frac{4c^2(1-2n)^2 n^2(-\beta\theta c_a(\beta\omega+T)+\beta l n\omega c_p+1)^2}{((n-1)(2n-1)\bar{a}+(3n-1)\underline{a})^2}\right)}{4\beta c\theta l n(2n-1)c_a}$. The expression is always positive given all constraints. Therefore, we conclude that $\frac{d\Pi}{d\bar{a}} < \frac{d\Pi}{d\underline{a}} < 0$.

Let us now discuss part (ii) of Proposition 3.4.3. We define that $B_1 = (-6n^2 + 4n - 1)$ $B_2 = \underline{a}B_1 (\beta^2\theta\omega c_a + \beta\theta T c_a + \beta l(2n(9n-7) + 3)n\omega c_p - 1) + (1-2n)^2\bar{a}(\beta\theta c_a(\beta\omega+T) + \beta l n(2n-3)\omega c_p - 1)$. Derivative of the total cost (1) with respect to the number of participants (i.e., n) is given as

$$\frac{d\Pi^*}{dn} = \frac{\frac{4cB_2(\beta\theta c_a(\beta\omega+T)-\beta l n\omega c_p-1)}{\beta l c_a((n-1)(2n-1)\bar{a}+(3n-1)\underline{a})^2} + \frac{\beta l c_a((1-2n)^2(-\bar{a})+2n(3n-2)\underline{a}+\underline{a})}{c(1-2n)^2 n^2} + 4\beta l\omega c_p}{8\theta}. \quad (9)$$

Furthermore, we can write the threshold value for θ as

$$\hat{\theta}_2 = \frac{2\left(\frac{l n\omega c_p\left((2(7-9n)n-3)\underline{a}-(1-2n)^2(2n-3)\bar{a}\right) + \frac{1}{\beta}}{B_1\underline{a}+(1-2n)^2\bar{a}}\right) + \frac{l((n-1)(2n-1)\bar{a}+(3n-1)\underline{a})}{cn(2n-1)}}{c_a} + \frac{l((n-1)(2n-1)\bar{a}+(3n-1)\underline{a})}{cn(2n-1)}. \quad (10)$$

Upon examination of the derivative $\frac{d\Pi^*}{dn}$ (9) and the threshold (10), we find that the threshold and $(-6n^2 + 4n - 1)\underline{a} + (1 - 2n)^2\bar{a}$ jointly determine the sign of the derivative. Specifically, $\frac{d\Pi^*}{dn} > 0$ when $(-6n^2 + 4n - 1)\underline{a} + (1 - 2n)^2\bar{a} > 0$ (i.e., high heterogeneity of security researchers' productivity) and $\theta < \hat{\theta}_2$. Furthermore, $\frac{d\Pi^*}{dn} > 0$ if $(-6n^2 + 4n - 1)\underline{a} + (1 - 2n)^2\bar{a} < 0$ (i.e., low heterogeneity of security researchers' productivity). Hence the proof. \blacksquare

Proofs of Proposition 3.4.4

We first discuss part (i) of Proposition 3.4.4. Derivative of the optimal bounty with respect to the legal protection is given by

$$\frac{db^*}{dl} = -\frac{cn(2n-1)(\beta\theta c_a(\beta\omega+T)-1)}{\beta\theta l^2 c_a((n-1)(2n-1)\bar{a}+(3n-1)\underline{a})}. \quad (11)$$

Upon examination of (11), we write the threshold value for c_a as $\frac{1}{\beta\theta(\beta\omega+T)}$. Therefore, $\frac{db^*}{dl} > 0$ when $c_a > \frac{1}{\beta\theta(\beta\omega+T)}$. Otherwise, $\frac{db^*}{dl} < 0$. Therefore, we conclude that the optimal bounty increases in the legal protection when the coefficient of the damage cost is large.

Now let us discuss part (ii) of Proposition 3.4.4. Derivative of the optimal bounty with respect to the legal protection is given by

$$\frac{d\Pi^*}{dl} = \frac{\frac{4cn(2n-1)(\beta\theta c_a(\beta\omega+T)-\beta l n \omega c_p - 1)(\beta\theta c_a(\beta\omega+T)+\beta l n \omega c_p - 1)}{\beta l^2 c_a((n-1)(2n-1)\bar{a}+(3n-1)\underline{a})} + \frac{\beta c_a(((3-2n)n-1)\bar{a}-3n\underline{a}+a)}{cn(2n-1)} + 4\beta n \omega c_p}{8\theta}. \quad (12)$$

The sign of (12) is determined by $4\beta^2 l^2 c((2n-1)n^2 \omega c_a c_p((n-1)(2n-1)\bar{a}+(3n-1)\underline{a}) - \beta^2 l^2 c_a^2((n-1)(2n-1)\bar{a}+(3n-1)\underline{a})^2 + 4c^2(1-2n)^2 n^2(\beta\theta c_a(\beta\omega+T) - \beta l n \omega c_p - 1)(\beta\theta c_a(\beta\omega+T) + \beta l n \omega c_p - 1)$.

Upon the examination of the equation, we can write the threshold value for c_p as $\frac{c_a((n-1)\bar{a} + \frac{a-3n\underline{a}}{1-2n})}{2cn^2\omega} - \frac{\beta\theta c_a(\beta\omega+T)-1}{\beta l n \omega}$. As a result, the $\frac{d\Pi^*}{dl} < 0$ when $c_p < \frac{c_a((n-1)\bar{a} + \frac{a-3n\underline{a}}{1-2n})}{2cn^2\omega} - \frac{\beta\theta c_a(\beta\omega+T)-1}{\beta l n \omega}$. Otherwise, $\frac{d\Pi^*}{dl} > 0$ when $c_p > \frac{c_a((n-1)\bar{a} + \frac{a-3n\underline{a}}{1-2n})}{2cn^2\omega} - \frac{\beta\theta c_a(\beta\omega+T)-1}{\beta l n \omega}$. Hence the proof. ■

B.2 Extension 1: Strategic Hacker

The strategic hacker's strategy set $H = \{Attack, NotAttack\}$. He or she attacks the organization only when (i) $a_h r_h - \gamma > 0$, implying that the marginal benefit exceed the marginal cost) and (ii) $\mathbb{E}[L - T + a_h e_h] = \mathbb{E}[I + \beta\omega] - T + a_h e_h > 0$, indicating that the duration of the hacker' attacking should be positive.

If the strategic hacker attacks the organization, the objective function of the organization is

$$\begin{aligned} \Pi = & \beta(1 - b\theta)c_h \left(\frac{bl(((3 - 2n)n - 1)\bar{a} - 3n\underline{a} + \underline{a})}{2cn(2n - 1)} + a_h e_h + \beta\omega \right) \\ & + \beta c_a(1 - b\theta) \left(\frac{bl(((3 - 2n)n - 1)\bar{a} - 3n\underline{a} + \underline{a})}{2cn(2n - 1)} + \beta\omega + T \right) + \beta bln\omega c_p + b \end{aligned} \quad (13)$$

If the strategic hacker does not attack the organization, the objective function is the same as (1).

Given (13), we can solve the equilibrium bounty in the attacking case. The first-order derivative reveals that

$$\begin{aligned} \frac{\partial \Pi}{\partial b} = & \frac{\beta l(2b\theta - 1) ((n - 1)(2n - 1)\bar{a} + (3n - 1)\underline{a})(c_a + c_h)}{2cn(2n - 1)} \\ & - \beta(\theta a_h c_h e_h + \beta\theta\omega(c_a + c_h) + \theta T c_a - ln\omega c_p) + 1. \end{aligned}$$

The second-order derivative can be written as $\frac{\partial^2 \Pi}{\partial b^2} = \frac{\beta\theta l((n-1)(2n-1)\bar{a} + (3n-1)\underline{a})(c_a + c_h)}{cn(2n-1)}$. It is always positive given feasible constraints, suggesting that the solution of the first-order equation is the optimal bounty (i.e., minimizes the total cost). Therefore, we solve the equation and write the optimal bounty as

$$b_h^* = \frac{\frac{2cn(2n-1)(\beta(\theta a_h c_h e_h + \beta\theta\omega(c_a + c_h) + \theta T c_a - ln\omega c_p) - 1)}{\beta l((n-1)(2n-1)\bar{a} + (3n-1)\underline{a})(c_a + c_h)} + 1}{2\theta}. \quad (14)$$

Plugging (14) into (13), the equilibrium total cost can be written as

$$\begin{aligned} \Pi_h^* = & \frac{1}{4\theta} \left(-\frac{2cn(2n-1)(\beta(\theta a_h c_h e_h + \beta\theta\omega(c_a + c_h) + \theta T c_a - ln\omega c_p) - 1)^2}{\beta l((n-1)(2n-1)\bar{a} + (3n-1)\underline{a})(c_a + c_h)} \right. \\ & \left. \frac{\beta l((n-1)(2n-1)\bar{a} + (3n-1)\underline{a})(c_a + c_h)}{2cn(2n-1)} + 2\beta(\theta a_h c_h e_h + \beta\theta\omega(c_a + c_h) + \theta T c_a + ln\omega c_p) + 2 \right) \end{aligned} \quad (15)$$

Counterpart of Proposition 3.4.1

We first prove the counterpart of part (i) of Proposition 3.4.1. Derivative of the equilibrium bounty (14) with respect to the patching time is given as:

$\frac{db^*}{d\omega} = \frac{cn(2n-1)(\beta\theta(c_a+c_h)-lnc_p)}{\theta l((n-1)(2n-1)\bar{a}+(3n-1)\underline{a})(c_a+c_h)}$. Given the feasibility condition, $\frac{db^*}{d\omega} > 0$ or $\frac{db^*}{d\omega} < 0$.

Hence the proof. \blacksquare

Let us prove the counterpart of part (ii) of Proposition 3.4.1. Derivative of the equilibrium bounty (14) with respect to the security posture is given as:

$\frac{db^*}{d\beta} = \frac{cn(2n-1)(\beta^2\theta\omega(c_a+c_h)+1)}{\beta^2\theta l((n-1)(2n-1)\bar{a}+(3n-1)\underline{a})(c_a+c_h)}$. Given the feasibility condition, $\frac{db^*}{d\beta} > 0$. Hence the proof. \blacksquare

Counterpart of Proposition 3.4.2

We first prove the counterpart of part (i) of Proposition 3.4.2. Derivative of the equilibrium bounty (14) with respect to the lower bound of the productivity \underline{a} is given as:

$\frac{db^*}{d\underline{a}} = -\frac{cn(2n-1)(3n-1)(\beta(\theta a_h c_h e_h + \beta\theta\omega(c_a+c_h) + \theta T c_a - l n \omega c_p) - 1)}{\beta\theta l((n-1)(2n-1)\bar{a} + (3n-1)\underline{a})^2(c_a+c_h)}$. Given the feasibility conditions, it is straightforward to show that $\frac{d(b^*)}{d\underline{a}} > 0$ or $\frac{d(b^*)}{d\underline{a}} < 0$.

Next, we prove the counterpart of part (ii) of Proposition 3.4.2. Derivative of the equilibrium bounty (14) with respect to the upper bound of the productivity \bar{a} is given as: $\frac{db^*}{d\bar{a}} = -\frac{c(1-2n)^2(n-1)n(\beta(\theta a_h c_h e_h + \beta\theta\omega(c_a+c_h) + \theta T c_a - l n \omega c_p) - 1)}{\beta\theta l((n-1)(2n-1)\bar{a} + (3n-1)\underline{a})^2(c_a+c_h)}$. Given the feasibility conditions, it is straightforward to show that $\frac{d(b^*)}{d\bar{a}} > 0$ or $\frac{d(b^*)}{d\bar{a}} < 0$. Hence the proof.

We first prove the counterpart of part (ii) of Proposition 3.4.2. We define that $C_1 = c\underline{a}(\beta\theta(6n^2 - 4n + 1)(a_h c_h e_h + T c_a))$. Derivative of the equilibrium bounty (14)

with respect to the number of security researchers n is given as:

$$\frac{db^*}{dn} = \frac{C_1 + \beta^2\theta(6n^2 - 4n + 1)\omega(c_a + c_h) + \beta l(3(3 - 4n)n - 2)n\omega c_p - 6n^2 + 4n - 1}{\beta\theta l((n-1)(2n-1)\bar{a} + (3n-1)\underline{a})^2(c_a + c_h)} - \frac{(1-2n)^2\bar{a}(\beta(\theta a_h c_h e_h + \beta\theta\omega(c_a + c_h) + \theta T c_a + l(n-2)n\omega c_p) - 1)}{\beta\theta l((n-1)(2n-1)\bar{a} + (3n-1)\underline{a})^2(c_a + c_h)}$$

Given the feasibility conditions, it is straightforward to show that $\frac{db^*}{dn} > 0$ or $\frac{db^*}{dn} < 0$. Hence the proof. \blacksquare

Counterpart of Proposition 3.4.3

We first prove the counterpart of part (i) of Proposition 3.4.3. Derivative of the equilibrium total cost (15) with respect to the lower bound of the productivity or the upper bound of the productivity \underline{a} is given as:

$$\frac{d\Pi^*}{d\underline{a}} = \frac{(3n-1)(4c^2(1-2n)^2n^2(\beta\theta a_h c_h e_h + \beta\theta\omega(c_a + c_h) + \theta Tc_a - \ln\omega c_p ght) - 1)^2 - \beta^2 l^2 ((n-1)(2n-1)\bar{a} + (3n-1)\underline{a})^2 (c_a + c_h)^2}{8\beta c\theta l n(2n-1)((n-1)(2n-1)\bar{a} + (3n-1)\underline{a})^2 (c_a + c_h)}$$

$$\frac{d\Pi^*}{d\bar{a}} = \frac{(n-1)(4c^2(1-2n)^2n^2(\beta\theta a_h c_h e_h + \beta\theta\omega(c_a + c_h) + \theta Tc_a - \ln\omega c_p) - 1)^2 - \beta^2 l^2 ((n-1)(2n-1)\bar{a} + (3n-1)\underline{a})^2 (c_a + c_h)^2}{8\beta c\theta l n((n-1)(2n-1)\bar{a} + (3n-1)\underline{a})^2 (c_a + c_h)}$$

Given the feasibility conditions, it is straightforward to show that $\frac{d\Pi^*}{d\bar{a}} < \frac{d\Pi^*}{d\underline{a}} < 0$. Hence the proof.

Let us prove the counterpart of part (ii) of Proposition 3.4.3. Derivative of the equilibrium total cost (15) with respect to the total number of security researchers n is given as:

$$\frac{d\Pi^*}{dn} = -\frac{E_1 \beta l (n-1)(2n-1)\bar{a} + (3n-1)\underline{a} - 6n^2 + 4n - 1}{8\beta c\theta l (1-2n)^2 n^2 (n-1)(2n-1)\bar{a} + (3n-1)\underline{a})^2 c_a + c_h} + \frac{(1-2n)^2 \bar{a} c_a + c_h - 2cn(2n-1)E_2}{8\beta c\theta l (1-2n)^2 n^2 (n-1)(2n-1)\bar{a} + (3n-1)\underline{a})^2 c_a + c_h}$$

where $E_1 = \beta l(n-1)(2n-1)\bar{a} + (3n-1)\underline{a})c_a + c_h - 2cn(2n-1)1 - \beta\theta a_h c_h e_h + \beta\theta\omega c_a + c_h + \theta Tc_a - \ln\omega c_p$ and $E_2 = \underline{a} - \beta E_3 - \beta^2\theta 6n^2 - 4n + 1)\omega c_a + c_h + 6n^2 - 4n + 1 + (1-2n)^2 \bar{a}\beta\theta a_h c_h e_h + \beta\omega c_a + c_h + Tc_a + \beta \ln(2n-3)\omega c_p - 1$, and $E_3 = \theta 6n^2 - 4n + 1)a_h c_h e_h + Tc_a + \ln(2(7-9n)n-3)\omega c_p$.

Given the feasibility conditions, it is straightforward to show that $\frac{d\Pi^*}{dn} < 0$ or $\frac{d\Pi^*}{dn} > 0$. Hence the proof. ■

Counterpart of Proposition 3.4.4

We first prove the counterpart of part (i) of Proposition 3.4.4. Derivative of the equilibrium bounty (14) with respect to the legal protection l is given as:

$$\frac{db^*}{dl} = -\frac{cn(2n-1)\beta\theta a_h c_h e_h + \beta\omega c_a + c_h + Tc_a - 1}{\beta\theta l^2 (n-1)(2n-1)\bar{a} + (3n-1)\underline{a})c_a + c_h}$$

Given the feasibility constraints, $\frac{db^*}{dl} > 0$ or $\frac{db^*}{dl} < 0$. Hence the proof.

Let us prove the counterpart of part (ii) of Proposition 3.4.4. Derivative of the equilibrium total cost (15) with respect to the legal protection l is given as:

$$\frac{d\Pi^*}{dl} = \frac{4c(2n-1)n^2 F_1}{l^2((n-1)(2n-1)\bar{a} + (3n-1)\underline{a})(c_a + c_h)} - \frac{\beta^2((n-1)(2n-1)\bar{a} + (3n-1)\underline{a})(c_a + c_h)}{c(2n-1)} + 4\beta^2 n^2 \omega c_p$$

where $F_1 = (\beta(\theta a_h c_h e_h + \beta \theta \omega(c_a + c_h) + \theta T c_a - \ln \omega c_p) - 1)(\beta(\theta a_h c_h e_h + \beta \theta \omega(c_a + c_h) + \theta T c_a + \ln \omega c_p) - 1)$. Given the feasibility constraints, $\frac{d\Pi^*}{dt} > 0$ or $\frac{d\Pi^*}{dt} < 0$. Hence the proof. \blacksquare

B.3 Extension 2: Endogenize Security Posture

In this extension, we endogenize the patching time and consider explicitly that it is another decision variable. The objective function in this case can be written as:

$$\min_{b, \beta} \mathbb{E}[\Pi] = b + \int_0^{\mathbb{E}[I] + \omega\beta} c_a \beta (1 - \theta b) dt + \int_{\mathbb{E}[I]}^{\mathbb{E}[I] + \omega\beta} c_p b n l dt + (1 - \beta)^2 \zeta$$

where there are two decision variables (i.e., b and β). The first order conditions reveal the following:

$$\frac{\partial \Pi}{\partial b} = \frac{\beta l c_a (2b\theta - 1) ((n-1)(2n-1)\bar{a} + (3n-1)\underline{a})}{2cn(2n-1)} - \beta \theta c_a (\beta \omega + T) + \beta \ln \omega c_p + 1 \quad (16)$$

$$\frac{\partial \Pi}{\partial \beta} = c_a (1 - b\theta) \left(\frac{bl((3-2n)n-1)\bar{a} - 3n\underline{a} + \underline{a}}{2cn(2n-1)} + \beta \omega + T \right) + \beta \omega c_a (1 - b\theta) + b \ln \omega c_p + 2(1 - \beta)\zeta \quad (17)$$

To obtain the optimal level of two decision variables, we need to solve the system of equation $\begin{cases} \frac{\partial \Pi}{\partial b} = 0 \\ \frac{\partial \Pi}{\partial \beta} = 0 \end{cases}$. However, the system of equation cannot be explicitly solved to yield closed-form solutions. Therefore, we use implicit function theorem (IFT) to glean results and managerial insights.

Specifically, we check the robustness of our key propositions in Section 3.4 to this extension. Note that after getting the specific derivatives (by invoking the implicit function theorem), we prove the existence of numerical examples for each parts of the propositions that are non-monotone. Therefore, we prove the counterparts of the propositions for the extension model too. However, for propositions that are monotone, such an approach is not feasible. Hence, we conduct extensive numerical studies and do not observe any contradictions to those results.

Counterpart of Proposition 3.4.1

First, we denote (16) as $f(b)$ and (17) as $g(\beta)$. The optimal bounty b^* and optimal security posture β^* need to satisfy $f(b, \beta) = 0$ and $g(b, \beta) = 0$. Hence, we obtain $\beta(b)$ by solving $g(b, \beta) = 0$ and plug $\beta(b)$ into $f(b, \beta) = 0$. Therefore, we can obtain $f(b) = 0$. Next, we prove the counterpart of part (i) of Proposition 3.4.1. Based on the $f(b)$, we can derive that

$$\begin{aligned} \frac{\partial f(b)}{\partial b} = & \frac{1}{A_3} (-4A_1 c^2 l (1-2n)^2 n^2 c_a (-A_2 \theta \omega^3 c_a (\omega c_a (b\theta - 3)(b\theta - 1) + \zeta(3-4b\theta)) + 4\zeta^2 \omega c_a (\theta(b^2 \theta (\theta c_a (3T + \omega) - 3 \ln \omega c_p - 5) \\ & + b(-4\theta T c_a + 2 \ln \omega c_p + 8) + c_a(T - \omega) - 3) + 4\zeta^3 (2b\theta - 1)(\theta \omega c_a + 1) + \omega^2 c_a^3 (b\theta - 1)^2 (2\omega(b\theta(b\theta - 2)(\ln T c_p - 2) \\ & - 2) - \theta T^2 c_a (b\theta - 1)^2) + \zeta \omega c_a^2 (b\theta - 1)(\theta T c_a (b\theta - 1)(T(4b\theta - 1) + 4\omega) + 4\omega(b\theta(-2b\theta(\ln T c_p - 2) + \ln c_p(T - 2\omega) \\ & - 7) + 3))) + A_1^3 b^2 \theta l^3 \omega c_a^4 (b\theta - 1)^2 (\omega c_a (b\theta - 1)^2 - 2b\zeta\theta + \zeta) + 8c^3 n^3 (2n-1)^3 (-\ln \omega^2 c_a c_p + \zeta \theta c_a (T + 2\omega) - \zeta \ln \omega c_p) + \\ & (A_2 \theta \omega^3 c_a + \omega c_a^2 (b\theta - 1)(\theta T^2 c_a (b\theta - 1) - 2\omega(b\theta(\ln T c_p - 2) + 2)) + 4\zeta \omega c_a ((b\theta - 1)(\theta T c_a - 2) - b\theta \ln \omega c_p) + \\ & 4\zeta^2 (\theta \omega c_a + 1)) + 2A_1^2 b c \theta l^2 n (2n-1) \omega c_a^3 (b\theta - 1) (\omega c_a (b \ln \omega (b\theta - 1)(2b\theta - 3) c_p - 2T c_a (b\theta - 1)^3) + \zeta c_a (b\theta - 1) \\ & (-2b\theta \omega + 5b\theta T - 2T + 4\omega) + b\zeta \ln \omega (3 - 5b\theta) c_p + \zeta^2 (8b\theta - 4))). \\ & \text{where } A_1 = 2n^2 \bar{a} - 3n\bar{a} + 3n\underline{a} + \bar{a} - \underline{a}, A_2 = b^2 l^2 n^2 c_p^2, A_3 = 4b^2 \theta l^3 n^2 c_a c_p^2 (\omega c_a (1 - b\theta) + \zeta)^2 (b^3 l^3 n^2 c_a \\ & (b\theta - 1) c_p^2 + 2cn(2n-1)(-b\theta T c_a + T c_a + b \ln \omega c_p - 2\zeta))^2 \end{aligned} \quad (18)$$

$$\begin{aligned} \frac{\partial f(b)}{\partial \omega} = & \frac{1}{B_4} (-b^3 B_1^3 \zeta \theta l^3 c_a^4 (b\theta - 1)^3 - 8c^3 n^3 (2n-1)^3 (-2\zeta c_a (b^2 l^3 n^3 \omega^3 (b\theta - 2) c_p^3 - 4\zeta^2 (b\theta(\ln T c_p - 1) - \ln c_p(T - 2\omega) + 1) + \\ & b\zeta \ln \omega c_p (b\theta(\ln c_p(2T - 3\omega) + 4) - 2 \ln c_p(T - 4\omega) - 4) + 4\zeta^3 \theta) - 2c_a^3 (b\theta - 1)^2 (bl^2 n^2 T \omega^3 (b\theta - 2) c_p^2 - 2\zeta \omega (b\theta T (\ln \omega c_p + 2) - \\ & 2\omega(b\theta - 1) + \ln T^2 c_p - 2T(\ln \omega c_p + 1)) + 3\zeta^2 \theta T^2) + T c_a^4 (b\theta - 1)^3 (\omega^2 (b\theta(\ln T c_p - 4) - 2 \ln T c_p + 4) - \zeta \theta T^2) + 2\zeta^2 \ln c_p (b^2 l^2 n^2 \omega^2 c_p^2 + \\ & b\zeta(2 - 4 \ln \omega c_p) + 4\zeta^2) + B_3) - 2b^2 B_1^2 B_2 c l^2 n (2n-1) c_a^2 (b\theta - 1)^2 - 4b B_1 c^2 l (1-2n)^2 n^2 c_a (b\theta - 1) (2c_a^2 (b\theta - 1) \\ & (bl^2 n^2 \omega^3 (b\theta - 2) c_p^2 - 2\zeta \omega (b\theta(\ln \omega c_p + 2) + 2 \ln c_p(T - \omega) - 2) + 6\zeta^2 \theta T) + \zeta c_a (bl^2 n^2 \omega^2 (8 - 3b\theta) c_p^2 - 4\zeta (b\theta(\ln T c_p - 1) - \ln c_p(T - 4\omega) + 1) + \\ & 12\zeta^2 \theta) + c_a^3 (b\theta - 1)^2 (3\zeta \theta T^2 - 2\omega^2 (b\theta(\ln T c_p - 2) - 2 \ln T c_p + 2)) + 4\zeta^2 \ln c_p (b \ln \omega c_p - 2\zeta))). \\ & \text{where } B_1 = 2n^2 \bar{a} - 3n\bar{a} + 3n\underline{a} + \bar{a} - \underline{a}, \\ & B_2 = \ln c_p (\omega^2 c_a^2 (b^2 \theta^2 - 3b\theta + 2) + 4\zeta \omega c_a + 2\zeta^2) - 3\zeta \theta c_a (T c_a (b\theta - 1) + 2\zeta), \\ & B_3 = c_a^2 (b\theta - 1) (b^2 l^3 n^3 \omega^4 (b\theta - 2) c_p^3 + 2\zeta^2 (2b\theta \omega (\ln \omega c_p + 4) + \ln T^2 (b\theta - 1) c_p + T(-2b\theta + 8 \ln \omega c_p + 2) - 4\omega (\ln \omega c_p + 2)) + \\ & b\zeta \ln \omega^2 c_p (b\theta(\ln c_p(3T - 4\omega) + 4) + 8 \ln c_p (\omega - T) - 4) - 12\zeta^3 \theta T), \\ & B_4 = 4B_1 \theta l c_a (\omega c_a (1 - b\theta) + \zeta)^2 (b B_1 l c_a (b\theta - 1) + 2cn(2n-1)(c_a (T - b\theta T) + b \ln \omega c_p - 2\zeta))^2. \end{aligned}$$

According to IFT, $\frac{\partial b^*}{\partial \beta} = -\frac{\frac{\partial f(b)}{\partial \omega}}{\frac{\partial f(b)}{\partial b}}$. Our numerical examples present that $\frac{\partial b^*}{\partial \beta}$ could be positive or negative. Hence the proof. ■

Counterpart of Proposition 3.4.2

We first prove the counterpart of part (i) of Proposition 3.4.2.

$$\begin{aligned} \frac{\partial f(b)}{\partial \underline{a}} &= \frac{1}{C_4} (-cn(6n^2 - 5n + 1)(4c^2(1 - 2n)^2 n^2 (\omega c_a (bln\omega^2 c_a (b\theta - 1) c_p (b\theta(3lnTc_p - 4) - 4lnTc_p + 4) - T\omega c_a^2 (b\theta - 1)^2 (b\theta(3lnTc_p - 4) - 2lnTc_p + 4) + \\ &\quad \theta T^3 c_a^3 (b\theta - 1)^3 + b^2 l^3 n^3 \omega^3 (2 - b\theta) c_p^3) - 2\zeta(\omega c_a^2 (b\theta - 1)(lnT^2(1 - 3b\theta) c_p + 2b\theta T(ln\omega c_p + 2) - 4\omega(b\theta - 1) - 4T(ln\omega c_p + 1))) + \\ &\quad bln\omega^2 c_a c_p (b\theta(lnc_p(3T - \omega) - 4) - 2ln c_p(T - 2\omega) + 4) + \theta T^2 c_a^3 (b\theta - 1)^2 (T - \omega) - b^2 l^3 n^3 \omega^3 c_p^3) - 8\zeta^3(\theta c_a(T + \omega) - \\ &\quad ln\omega c_p - 1) - 4c_3 \zeta^2) - b^2 C_1^2 l^2 c_a^2 (b\theta - 1)^2 (ln\omega^2 c_a (b\theta - 2) c_p + \theta T\omega c_a^2 (1 - b\theta) + 2\zeta\theta c_a(T + \omega) - 2\zeta ln\omega c_p) - 4bcC_1 C_2 l(2n - 1)nc_a(b\theta - 1))). \\ C_1 &= 2n^2 \underline{a} - 3n\underline{a} + 3n\underline{a} + \underline{a} - \underline{a} \\ C_2 &= -2\zeta(\omega c_a(-2b\theta(lnTc_p - 2) + lnc_p(T - 2\omega) - 4) + \theta T^2 c_a^2 (b\theta - 1) + bl^2 n^2 \omega^2 c_p^2) + \\ &\quad \omega c_a(-2\omega c_a(b\theta - 1)^2 (lnTc_p - 2) + \theta T^2 c_a^2 (b\theta - 1)^2 + bl^2 n^2 \omega^2 (b\theta - 2) c_p^2) - 4\zeta^2(\theta c_a(T + \omega) - ln\omega c_p - 1) \\ C_3 &= c_a(\omega(b\theta(ln\omega c_p - 4) + 2ln\omega c_p + 4) + T(b(4\theta ln\omega c_p + \theta) - 2ln\omega c_p - 1)) + \theta T c_a^2 (b\theta - 1)(2T + \omega) + bln\omega c_p(2ln\omega c_p + 1). \end{aligned}$$

$$\begin{aligned} \frac{\partial f(b)}{\partial \bar{a}} &= \frac{1}{D_4} (-c(1 - 2n)^2 (n - 1)n(4c^2(1 - 2n)^2 n^2 (\omega c_a (bln\omega^2 c_a (b\theta - 1) c_p (b\theta(3lnTc_p - 4) - 4lnTc_p + 4) - \\ &\quad T\omega c_a^2 (b\theta - 1)^2 (b\theta(3lnTc_p - 4) - 2lnTc_p + 4) + \theta T^3 c_a^3 (b\theta - 1)^3 + b^2 l^3 n^3 \omega^3 (2 - b\theta) c_p^3) - 4\zeta^2(-c_a(\omega(b\theta(ln\omega c_p - 4) + 2ln\omega c_p + 4) + \\ &\quad T(b(4\theta ln\omega c_p + \theta) - 2ln\omega c_p - 1)) + \theta T c_a^2 (b\theta - 1)(2T + \omega) + bln\omega c_p(2ln\omega c_p + 1)) - 8\zeta^3(\theta c_a(T + \omega) - \\ &\quad ln\omega c_p - 1) - 2D_3 \zeta) - b^2 D_1^2 l^2 c_a^2 (b\theta - 1)^2 (ln\omega^2 c_a (b\theta - 2) c_p + \theta T\omega c_a^2 (1 - b\theta) + 2\zeta\theta c_a(T + \omega) - 2\zeta ln\omega c_p) - 4bcD_1 D_2 l(2n - 1)nc_a(b\theta - 1))). \\ D_1 &= 2n^2 \bar{a} - 3n\bar{a} + 3n\underline{a} + \bar{a} - \underline{a}, \\ D_2 &= -2\zeta(\omega c_a(-2b\theta(lnTc_p - 2) + lnc_p(T - 2\omega) - 4) + \theta T^2 c_a^2 (b\theta - 1) + bl^2 n^2 \omega^2 c_p^2) + \omega c_a(-2\omega c_a(b\theta - 1)^2 (lnTc_p - 2) + \\ &\quad \theta T^2 c_a^2 (b\theta - 1)^2 + bl^2 n^2 \omega^2 (b\theta - 2) c_p^2) - 4\zeta^2(\theta c_a(T + \omega) - ln\omega c_p - 1), \\ D_3 &= \omega c_a^2 (b\theta - 1)(lnT^2(1 - 3b\theta) c_p + 2b\theta T(ln\omega c_p + 2) - \\ &\quad 4\omega(b\theta - 1) - 4T(ln\omega c_p + 1)) + bln\omega^2 c_a c_p (b\theta(lnc_p(3T - \omega) - 4) - 2ln c_p(T - 2\omega) + 4) + \theta T^2 c_a^3 (b\theta - 1)^2 (T - \omega) - b^2 l^3 n^3 \omega^3 c_p^3, \\ D_4 &= 2D_1^2 \theta l c_a (\omega c_a (b\theta - 1) - \zeta) (bD_1 l c_a (b\theta - 1) + 2cn(2n - 1)(c_a(T - b\theta T) + bln\omega c_p - 2\zeta))^2. \end{aligned}$$

According to IFT, $\frac{\partial b^*}{\partial \underline{a}} = -\frac{\frac{\partial f(b)}{\partial \underline{a}}}{\frac{\partial f(b)}{\partial b}}$ and $\frac{\partial b^*}{\partial \bar{a}} = -\frac{\frac{\partial f(b)}{\partial \bar{a}}}{\frac{\partial f(b)}{\partial b}}$. Our numerical examples present that $\frac{\partial b^*}{\partial \underline{a}}$ and $\frac{\partial b^*}{\partial \bar{a}}$ could be positive or negative. Hence the proof.

Next, we prove the counterpart of part (ii) of Proposition 3.4.2. According to IFT, $\frac{\partial b^*}{\partial n} = -\frac{\frac{\partial f(b)}{\partial n}}{\frac{\partial f(b)}{\partial b}}$ ($\frac{\partial f(b)}{\partial n}$ is on the next page).

$$\begin{aligned}
\frac{\partial f(b)}{\partial n} = & \frac{1}{F_6} c(4c^2(1-2n)^2(8(\bar{a}(\theta(T+\omega)c_a + l(n-2)n\omega c_p - 1)(1-2n)^2 + (12l\omega c_p n^3 - 3(2\theta(T+\omega)c_a + 3l\omega c_p - 2)n^2 + 2(2\theta(T+\omega)c_a + l\omega c_p - 2)n - \\
& \theta(T+\omega)c_a + 1)\underline{a})\zeta^3 + 4(bl\omega c_p(-\bar{a}(2l(n-2)\omega c_p - 1)(1-2n)^2 - (2l(12n^2 - 9n + 2)\omega c_p + 1)\underline{a})n^2 + T\theta(b\theta - 1)(2T+\omega)c_a^2(\bar{a}(1-2n)^2 + \\
& (-6n^2 + 4n - 1)\underline{a}) + c_a(\bar{a}(T - 2l(n-2)n\omega c_p + b\theta(2l(n-3)n\omega c_p - 1) + 1) - \omega(-2l(n-2)n\omega c_p + b\theta(ln^2\omega c_p - 4) + 4))(1-2n)^2 + F_5\underline{a})\zeta^2 + \\
& 2(T^2\theta(b\theta - 1)^2(T - \omega)(\bar{a}(1-2n)^2 + (-6n^2 + 4n - 1)\underline{a})c_a^3 + (b\theta - 1)\omega(\bar{a}(ln(-4b\theta + n(b\theta - 1) + 2)c_p T^2 + (4l(n-2)n\omega c_p + \\
& 2b\theta(2 - l(n-2)n\omega c_p) - 4)T - 4(b\theta - 1)\omega)(1-2n)^2 + (ln(12(2b\theta - 1)n^2 + (9 - 17b\theta)n + 4b\theta - 2)c_p T^2 - 2(12l(b\theta - 2)\omega c_p n^3 - 3(-6l\omega c_p + \\
& b\theta(3l\omega c_p - 4) + 4)n^2 + 2(-2l\omega c_p + b\theta(l\omega c_p - 4) + 4)n + 2b\theta - 2)T + 4(6n^2 - 4n + 1)(b\theta - 1)\omega)\underline{a})c_a^2 + bln^2\omega^2 c_p((2l(12n^2 - 9n + 2)(T - 2\omega)c_p + \\
& b\theta(l(-30n^2 + 22n - 5)T + (18n^2 - 14n + 3)\omega)c_p + 4) - 4)\underline{a} - (1-2n)^2\bar{a}(-2l(n-2)(T - 2\omega)c_p + b\theta(l(2nT - 5T - 2n\omega + 3\omega)c_p + 4) - 4))c_a + \\
& b^2 l^3 n^3 \omega^3 c_p^3 F_2)\zeta + \omega c_a(-T^3\theta(b\theta - 1)^3(\bar{a}(1-2n)^2 + (-6n^2 + 4n - 1)\underline{a})c_a^3 - T(b\theta - 1)^2\omega F_4 c_a^2 + bln^2(b\theta - 1)\omega^2 c_p(\bar{a}(-4l(n-2)Tc_p + \\
& b\theta(l(2n-5)Tc_p + 4) - 4)(1-2n)^2 + (-4l(12n^2 - 9n + 2)Tc_p + b\theta(l(30n^2 - 22n + 5)Tc_p - 4) + 4)\underline{a})c_a - b^2 l^3 n^3(b\theta - 2)\omega^3 c_p^3 F_2))n^2 - \\
& 4bcl(2n-1)(b\theta - 1)c_a F_1(4(\bar{a}(\theta(T+\omega)c_a + l(n-2)n\omega c_p - 1)(1-2n)^2 + (12l\omega c_p n^3 - 3(2\theta(T+\omega)c_a + 3l\omega c_p - 2)n^2 + \\
& 2(2\theta(T+\omega)c_a + l\omega c_p - 2)n - \theta(T+\omega)c_a + 1)\underline{a})\zeta^2 + 2(T^2\theta(b\theta - 1)(\bar{a}(1-2n)^2 + (-6n^2 + 4n - 1)\underline{a})c_a^2 + \omega(\bar{a}(-l(n-2)n(T - 2\omega)c_p + \\
& b\theta(ln((n-3)T - n\omega + \omega)c_p + 4) - 4)(1-2n)^2 + (6l(T(3b\theta - 2) + (4 - b\theta)\omega)c_p n^3 + (9l(T - 2\omega)c_p + b\theta(-13lTc_p + 5l\omega c_p - 24) + 24)n^2 + \\
& (b\theta(l(3T - \omega)c_p + 16) - 2l(T - 2\omega)c_p + 8))n - 4b\theta + 4)\underline{a})c_a + bl^2 n^2 \omega^2 c_p^2((-12n^2 + 9n - 2)\underline{a} - (1-2n)^2(n-2)\bar{a}))\zeta + \\
& \omega c_a(-T^2\theta(b\theta - 1)^2(\bar{a}(1-2n)^2 + (-6n^2 + 4n - 1)\underline{a})c_a^2 - (b\theta - 1)\omega F_3 c_a + bl^2 n^2(b\theta - 2)\omega^2 c_p^2 F_2))n - b^2 l^2(b\theta - 1)^2 c_a^2 F_1^2(T\theta(b\theta - 1) \\
& \omega(\bar{a}(1-2n)^2 + (-6n^2 + 4n - 1)\underline{a})c_a^2 + (ln(b\theta - 2)\omega^2 c_p F_2 - 2\zeta\theta(T+\omega)(\bar{a}(1-2n)^2 + (-6n^2 + 4n - 1)\underline{a}))c_a - 2ln\zeta\omega c_p F_2)). \\
F_1 = & 2n^2\bar{a} - 3n\bar{a} + 3n\underline{a} + \bar{a} - \underline{a} \\
F_2 = & (12n^2 - 9n + 2)\underline{a} + (n-2)(1-2n)^2\bar{a}, \\
F_3 = & \underline{a}(6ln^3 T(3b\theta - 4)c_p + n^2(6(3lTc_p + 4) - b\theta(13lTc_p + 24)) + n(b\theta(3lTc_p + 16) - 4(lTc_p + 4)) - 4b\theta + 4) + \\
& (1-2n)^2\bar{a}(b\theta(l(n-3)nTc_p + 4) - 2l(n-2)nTc_p - 4), \\
F_4 = & \underline{a}(24ln^3 T(b\theta - 1)c_p + n^2(6(3lTc_p + 4) - b\theta(17lTc_p + 24)) + 4n(b\theta - 1)(lTc_p + 4) - \\
& 4b\theta + 4) + (1-2n)^2\bar{a}(b\theta(l(n-4)nTc_p + 4) - 2l(n-2)nTc_p - 4), \\
F_5 = & \omega(n^2(b\theta(l\omega c_p - 24) - 18l\omega c_p + 24) + 4n(4b\theta + l\omega c_p - 4) - 4b\theta + 24ln^3\omega c_p + 4) + \\
& T(12ln^3\omega(3b\theta - 2)c_p + n^2(b\theta(6 - 26l\omega c_p) + 18l\omega c_p - 6) + n(2b\theta(3l\omega c_p - 2) - 4l\omega c_p + 4) + b\theta - 1), \\
F_6 = & 2F_1^2\theta l c_a(\omega c_a(b\theta - 1) - \zeta)(bF_1 l c_a(b\theta - 1) + 2cn(2n-1)(c_a(T - b\theta T) + bln\omega c_p - 2\zeta))^2.
\end{aligned}$$

Our numerical examples present that $\frac{\partial b^*}{\partial n}$ could be positive or negative. Hence the proof. ■

Counterpart of Proposition 3.4.3

The detailed proof are omitted for brevity.

Counterpart of Proposition 3.4.4

The detailed proof are omitted for brevity.

B.4 Extension 3: Multiple Vulnerabilities

We now examine the case when there are multiple independent (i.e., M) vulnerabilities in the BBP's targeted information system that could each be identified by

independent groups of security researchers. In this case, the objective function of the organization is:

$$\min_b \mathbb{E}[\Pi^M] = \sum_{m=1}^M b^m + \sum_{m=1}^M b^m \int_0^{\mathbb{E}[I^m] + \omega^m \beta} c_a^m \beta (1 - \theta b^m) dt + \sum_{m=1}^M b^m \int_{\mathbb{E}[I^m]}^{\mathbb{E}[I^m] + \omega^m \beta} c_p^m b^m n^m l dt \quad (19)$$

We take the derivative of (19) with respect to bounty b_m (where $m \in \{1, 2, \dots, M\}$). The set of first order conditions along with the non-negative nature of the bounty reveal that:

$$b^{m*} = \frac{1}{2\theta} - \frac{2c^m n^m (2n^m - 1) (-\beta \theta c_a^m (\beta \omega^m + T^m) + \beta \ln^m \omega^m c_p^m + 1)}{2\theta \beta l c_a^m ((n^m - 1)(2n^m - 1)\bar{a}^m + (3n^m - 1)\underline{a}^m)} \quad (20)$$

The second order conditions $\frac{\beta \theta l^m c_a^m ((n^m - 1)(2n^m - 1)\bar{a}^m + \underline{a}^m (3n^m - 1))}{c n^m (2n^m - 1)}$, $\forall m$ are satisfied for any set of feasible parameter values. Furthermore, the equilibrium values of the total cost for each vulnerability can be rewritten as:

$$\begin{aligned} \Pi^{m*} = & \frac{1}{8\theta} \left(\frac{\beta l c_a^m (((3 - 2n^m)n^m - 1)\bar{a}^m - 3n^m \underline{a}^m + \underline{a}^m)}{c^m n^m (2n^m - 1)} - \right. \\ & \frac{4c^m n^m (2n^m - 1) (-\beta \theta c_a^m (\beta \omega^m + T^m) + \beta \ln^m \omega^m c_p^m + 1)^2}{\beta l c_a^m ((n^m - 1)(2n^m - 1)\bar{a}^m + (3n^m - 1)\underline{a}^m)} + \\ & \left. 4\beta (\theta c_a^m (\beta \omega^m + T^m) + \ln^m \omega^m c_p^m) + 4 \right) \end{aligned} \quad (21)$$

The total cost of a BBP can be written as:

$$\begin{aligned} \Pi^{M*} = & \sum_{m=1}^M \left(\frac{1}{8\theta} \left(\frac{\beta l c_a^m (((3 - 2n^m)n^m - 1)\bar{a}^m - 3n^m \underline{a}^m + \underline{a}^m)}{c^m n^m (2n^m - 1)} - \right. \right. \\ & \frac{4c^m n^m (2n^m - 1) (-\beta \theta c_a^m (\beta \omega^m + T^m) + \beta \ln^m \omega^m c_p^m + 1)^2}{\beta l c_a^m ((n^m - 1)(2n^m - 1)\bar{a}^m + (3n^m - 1)\underline{a}^m)} + \\ & \left. \left. 4\beta (\theta c_a^m (\beta \omega^m + T^m) + \ln^m \omega^m c_p^m) + 4 \right) \right) \end{aligned} \quad (22)$$

Counterpart of Proposition 3.4.1

We first analyze the counterpart of part (i) of Proposition 3.4.1. We take derivative of the optimal bounty (20) with respect to the patching complexity ω and obtain $\frac{db^{m*}}{d\omega^m} = \frac{c^m n^m (2n^m - 1) (\beta \theta c_a^m - \ln^m c_p^m)}{\theta l c_a^m ((n^m - 1)(2n^m - 1)\bar{a}^m + (3n^m - 1)\underline{a}^m)}$. Given all constraints, $\frac{db^{m*}}{d\omega^m} > 0$ or $\frac{db^{m*}}{d\omega^m} < 0$.

Next, we discuss the counterpart of part (ii) of Proposition 3.4.1. Derivative of the optimal bounty (20) with respect to the security posture β is given by $\frac{db^{m*}}{d\beta} = \frac{c^m n^m (2n^m - 1) (\beta^2 \theta \omega^m c_a^m + 1)}{\beta^2 \theta l c_a^m ((n^m - 1)(2n^m - 1)\bar{a}^m + (3n^m - 1)\underline{a}^m)}$. Given all constraints, the derivative is always pos-

itive, suggesting that the optimal bounty always increase an organization's security posture. Hence the proof. ■

Counterpart of Proposition 3.4.2

We first prove the counterpart of part (i) of Proposition 3.4.2. Derivative of the equilibrium bounty (20) with respect to the bound of the productivity (i.e., \underline{a}^m , \bar{a}^m) is given as:

$$\frac{d(b^{m*})}{d\underline{a}^m} = \frac{c^m n^m (n^m (6n^m - 5) + 1) (-\beta \theta c_a^m (\beta \omega^m + T^m) + \beta l n^m \omega c_p^m + 1)}{\beta \theta l c_a^m ((n^m - 1)(2n^m - 1)\bar{a}^m + \underline{a}^m (3n^m - 1))^2},$$

$$\frac{db^{m*}}{d\bar{a}^m} = \frac{c^m (1 - 2n^m)^2 (n^m - 1) n^m (-\beta \theta c_a^m (\beta \omega^m + T^m) + \beta l n^m \omega c_p^m + 1)}{\beta \theta l c_a^m ((n^m - 1)(2n^m - 1)\bar{a}^m + \underline{a}^m (3n^m - 1))^2}.$$

Given the feasibility conditions, it is straightforward to show that $\frac{d(b^{m*})}{d\underline{a}^m} > 0$ or $\frac{d(b^{m*})}{d\underline{a}^m} < 0$, and $\frac{d(b^{m*})}{d\bar{a}^m} > 0$ or $\frac{d(b^{m*})}{d\bar{a}^m} < 0$. Hence the proof.

Let us now discuss the counterpart of part (ii) of the proposition. Derivative of the equilibrium bounty (20) with respect to the number of security researcher n is given as:

$$\frac{db^{m*}}{dn^m} = \frac{c^m (\underline{a}^m (\beta^2 \theta (6(n^m)^2 - 4n^m + 1) \omega^m c_a^m + \beta \theta (6(n^m)^2 - 4n^m + 1) T^m c_a^m + \beta l (3(3 - 4n^m)n^m - 2)n^m \omega^m c_p^m - 6(n^m)^2 + 4n^m))}{\beta \theta l c_a^m ((n^m - 1)(2n^m - 1)\bar{a}^m + (3n^m - 1)\underline{a}^m)^2} \frac{\beta l + G^m}{\beta \theta l c_a^m ((n^m - 1)(2n^m - 1)\bar{a}^m + (3n^m - 1)\underline{a}^m)^2}$$

where $G = (1 - 2n^m)^2 \bar{a}^m (\beta \theta c_a^m (\beta \omega^m + T^m) + \beta l (n^m - 2)n^m \omega^m c_p^m - 1)$.

Given the feasibility conditions, it is straightforward to show that $\frac{d(b^{m*})}{dn^m} > 0$ or $\frac{d(b^{m*})}{dn^m} < 0$. Hence the proof. ■

Counterpart of Proposition 3.4.3

Next, we discuss the counterpart of part (i) of Proposition 3.4.3. We take the derivative of the equilibrium total cost (22) with respect to \underline{a}^m and \bar{a}^m , obtaining

$$\frac{d\Pi^{M*}}{d\underline{a}^m} = \frac{4c^m n^m (n^m (6n^m - 5) + 1) (-\beta \theta c_a^m (\beta \omega^m + T^m) + \beta l n^m \omega c_p^m + 1)^2}{\beta l c_a^m ((n^m - 1)(2n^m - 1)\bar{a}^m + (3n^m - 1)\underline{a}^m)^2} + \frac{\beta l (1 - 3n^m) c_a^m}{c n^m (2n^m - 1)},$$

$$\frac{d\Pi^{M*}}{d\bar{a}^m} = \frac{4c^m (1 - 2n^m)^2 (n^m - 1) n^m (-\beta \theta c_a^m (\beta \omega^m + T^m) + \beta l n^m \omega c_p^m + 1)^2}{\beta l c_a^m ((n^m - 1)(2n^m - 1)\bar{a}^m + (3n^m - 1)\underline{a}^m)^2} - \frac{\beta l (n^m - 1) c_a^m}{c^m n^m}.$$

Both of the derivatives are always negative given constraints. The differences between the two marginal effects can be written as

$$\frac{d\Pi^{M*}}{d\bar{a}^m} - \frac{d\Pi^{M*}}{d\underline{a}^m} = \frac{((n^m - 3)n^m + 1) \left(\beta^2 l^2 (c_a^m)^2 - \frac{4(c^m)^2 (1-2n^m)^2 (n^m)^2 (-\beta\theta c_a^m (\beta\omega^m + T^m) + \beta l n^m \omega^m c_p^m + 1)^2}{((n^m - 1)(2n^m - 1)\bar{a}^m + (3n^m - 1)\underline{a}^m)^2} \right)}{4\beta c^m \theta l n^m (2n^m - 1) c_a^m}.$$

The expression is always positive given all constraints. Therefore, we conclude that $\frac{d\Pi^{M*}}{d\bar{a}^m} < \frac{d\Pi^{M*}}{d\underline{a}^m} < 0$.

Let us now discuss the counterpart of part (ii) of Proposition 3.4.3. Derivative of the total cost (22) with respect to the number of participants (i.e., n^m) is given as

$$\frac{d\Pi^{M*}}{dn^m} = \frac{\frac{4c^m G^m (\beta\theta c_a^m (\beta\omega^m + T^m) - \beta l n^m \omega^m c_p^m - 1)}{\beta l c_a^m ((n^m - 1)(2n^m - 1)\bar{a}^m + (3n^m - 1)\underline{a}^m)^2} + \frac{\beta l c_a^m ((1-2n^m)^2 (-\bar{a}^m) + 2n^m (3n^m - 2)\underline{a}^m + \underline{a}^m)}{c^m (1-2n^m)^2 (n^m)^2} + 4\beta l \omega^m c_p^m}{8\theta}$$

where $G = \underline{a}^m (\beta^2 \theta (-6(n^m)^2 + 4n^m - 1) \omega c_a^m + \beta \theta (-6(n^m)^2 + 4n^m - 1) T c_a^m + \beta l (2n^m (9n^m - 7) + 3)n^m \omega c_p^m + 6(n^m)^2 - 4n^m + 1) + (1 - 2n^m)^2 \bar{a}^m (\beta\theta c_a^m (\beta\omega^m + T^m) + \beta l n^m (2n^m - 3) \omega^m c_p^m - 1)$. Given the feasibility conditions, it is straightforward to show that $\frac{d\Pi^{M*}}{dn^m} > 0$ or $\frac{d\Pi^{M*}}{dn^m} < 0$. Hence the proof. \blacksquare

Counterpart of Proposition 3.4.4

We first discuss the counterpart of part (i) of Proposition 3.4.4. Derivative of the optimal bounty 20 with respect to the legal protection l is given by

$$\frac{db^{m*}}{dl} = - \frac{c^m n^m (2n^m - 1) (\beta\theta c_a^m (\beta\omega^m + T^m) - 1)}{\beta\theta l^2 c_a^m ((n^m - 1)(2n^m - 1)\bar{a}^m + (3n^m - 1)\underline{a}^m)}.$$

Given the feasibility conditions, it is straightforward to show that $\frac{db^{m*}}{dl} > 0$ or $\frac{db^{m*}}{dl} < 0$.

Now let us discuss the counterpart of part (ii) of Proposition 3.4.4. Derivative of the equilibrium total cost (22) with respect to the legal protection l is given by

$$\begin{aligned} \frac{d\Pi^{M*}}{dl} = & \frac{4c^m n^m (2n^m - 1) (\beta\theta c_a^m (\beta\omega^m + T^m) - \beta l n^m \omega^m c_p^m - 1) (\beta\theta c_a^m (\beta\omega^m + T^m) + \beta l n^m \omega^m c_p^m - 1)}{8\theta \beta l^2 c_a^m ((n^m - 1)(2n^m - 1)\bar{a}^m + (3n^m - 1)\underline{a}^m)} + \\ & \frac{\beta c_a^m (((3 - 2n^m)n^m - 1)\bar{a}^m - 3n^m \underline{a}^m + \underline{a}^m)}{8\theta c n^m (2n^m - 1)} + \\ & \frac{4\beta n^m \omega^m c_p^m}{8\theta}. \end{aligned}$$

Given the feasibility conditions, it is straightforward to show that $\frac{d\Pi^{M*}}{dl} > 0$ or $\frac{d\Pi^{M*}}{dl} < 0$. Hence the proof. \blacksquare

C APPENDIX - STUDY 3

Table C.1. Correlation Matrix

Variables	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
(1) CRD Quality	1.00							
(2) CRD Length	0.54	1.00						
(3) No. Peer Breaches	0.12	0.25	1.00					
(4) Other Risks Disclosures Length	0.33	0.32	0.05	1.00				
(5) Has Data Breach This Year	0.04	0.09	0.13	0.00	1.00			
(6) Total Asset	0.27	0.24	0.23	0.12	0.14	1.00		
(7) Intangible Asset	0.19	0.18	0.01	0.09	0.12	0.66	1.00	
(8) Operating Expenses	0.21	0.14	-0.15	0.07	0.15	0.76	0.68	1.00
(9) Book Value per Share	0.15	0.11	0.15	-0.00	0.04	0.57	0.32	0.41
(10) Employees	0.07	0.08	0.01	-0.11	0.20	0.39	0.34	0.48
(11) Market HHI	-0.18	-0.19	-0.36	-0.23	-0.04	-0.30	-0.04	-0.07
(12) Internal Weakness	-0.02	0.00	-0.04	0.03	-0.02	-0.10	-0.04	-0.07
(13) Public Attention on Data Breaches	0.06	0.30	0.11	0.07	0.03	-0.00	0.01	-0.02
(14) No. Sites	0.16	0.17	0.18	-0.03	0.13	0.67	0.57	0.62
(15) Installed Cybersecurity Apps	-0.02	-0.08	-0.01	-0.08	0.00	0.09	0.06	0.06
	(9)	(10)	(11)	(12)	(13)	(14)	(15)	
(9) Book Value per Share	1.00							
(10) Employees	0.10	1.00						
(11) Market HHI	-0.16	-0.00	1.00					
(12) Internal Weakness	-0.10	-0.03	0.07	1.00				
(13) Public Attention on Data Breaches	0.00	-0.01	-0.00	0.07	1.00			
(14) No. Sites	0.35	0.39	-0.12	-0.04	0.03	1.00		
(15) Installed Cybersecurity Apps	0.08	0.01	0.01	-0.03	-0.17	0.06	1.00	

Table C.2. Cybersecurity Keywords Used to Extract Cyber Risk Disclosure (CRD)

Data Threat, Computer Vulnerability, Cyber Vulnerability, Digital Vulnerability, Data Vulnerability, Computer Intrusion, Cyber Intrusion, Digital Intrusion, Data Intrusion, Network Intrusion, Cyber Assessment, Security Assessment, Cyber Investment, Security Investment, Cyber Expense, Security Expense, Digital Forensics, Encryption, Exploitation Analysis, Firewall, Hack, Phishing, Privacy Breach, Security Breach, Data Breach, Information Security, Network Security, Computer Security, Security Management, Hacker, Security Monitoring, Denial of Service, Cyber Attack, Security Incident, Infosec, Cybersecurity, Computer System Security, Computer Breach, Cyber Security

Table C.3. Cybersecurity Applications in CITDB

Firewall
Network Management
Backup and Recovery
Anti-Virus
Disaster Recovery
Security/Encryption
Identity Management
Access Management
Network Management Tools
Data Loss Prevention Software
Message Security Software
Email Anti-Virus
Network Management Software
Security Information & Event

REFERENCES CITED

- (2009) Do managers withhold bad news? *Journal of Accounting Research* 47(1):241–276.
- Abadie A, Athey S, Imbens G, Wooldridge J (2017) When Should You Adjust Standard Errors for Clustering?, Available at <http://arxiv.org/abs/1710.02926>.
- Acemoglu D, Malekian A, Ozdaglar A (2016) Network security and contagion. *Journal of Economic Theory* 166:536–585.
- Adjerid I, Adler-Milstein J, Angst CM (2018) Reducing Medicare Spending Through Electronic Information Exchange: The Role of Incentives and Exchange Maturity. *Information Systems Research* (Feb).
- Adler-Milstein J, DesRoches CM, Jha AK (2011) Health information exchange among US hospitals. *Am J Manag Care* 17(11):761–768.
- Adler-Milstein J, Jha AK (2014) Health information exchange among U.S. hospitals: Who’s in, who’s out, and why? *Healthcare* 2(1):26–32.
- Aghamolla C, Thakor RT (2022) IPO Peer Effects. *Journal of Financial Economics* 144(1):206–226.
- AHIMA/HIMSS (2011) The Privacy and Security Gaps in Health Information Exchanges. Technical report.
- AHRQ (2017) Defining Health Systems. Available at <https://www.ahrq.gov/chsp/chsp-reports/resources-for-understanding-health-systems/defining-health-systems.html>.
- Al-banna M, Schlagwein D, Bertino E, Barukh MC, Schlagwein D (2018) Friendly Hackers to the Rescue: How Organizations Perceive Crowdsourced Vulnerability Discovery. *PACIS 2018 Preceedings*, 230.
- Ales L, Cho SH, Körpeoğlu E (2019) Innovation and Crowdsourcing Contests. *Sharing Economy*, volume 6, 379–406 (Springer).
- Alomar N, Wijesekera P, Qiu E, Egelman S (2020) “You’ve Got Your Nice List of Bugs, Now What?” Vulnerability Discovery and Management Processes in the Wild. *Proceedings of the 16th Symposium on Usable Privacy and Security, SOUPS 2020* 319–340.
- Anantharaman D, Zhang Y (2011) Cover me: Managers’ responses to changes in analyst coverage in the post-regulation fd period. *Accounting Review* 86(6):1851–1885.
- Anderson R, Moore T (2006) The Economics of Information Security. *Science* .

- Andress J, Leary M (2016) *Building a Practical Information Security Program* (Syngress).
- Andrews M, Luo X, Fang Z, Aspara J (2014) Cause marketing effectiveness and the moderating role of price discounts. *Journal of Marketing* 78(6):120–142.
- Angrist JD, Krueger AB (2001) Instrumental Variables and the Search for Identification: From Supply and Demand to Natural Experiments. *Journal of Economic Perspectives* 15(4):69–85.
- Angrist JD, Pischke JS (2008) *Mostly Harmless Econometrics: An Empiricist's Companion* (Princeton university press.).
- Angst C, Wowak K, Handley S, Kelley K (2017) Antecedents of information systems sourcing strategies in U.S. hospitals: A longitudinal study. *MIS Quarterly* 41(4):1–18.
- Archak N, Sundararajan A (2009) Optimal Design of Crowdsourcing. *ICIS 2009 Proceedings*, 200.
- Arora A, Belenzon S, Sheer L (2021) Knowledge spillovers and corporate investment in scientific research. *American Economic Review* 111(3):871–898.
- Arora A, Telang R, Xu H (2008) Optimal Policy for Software Vulnerability Disclosure. *Management Science* 54(4):642–656.
- Ashraf M (2021) Should the SEC allow managers discretion when disclosing risk factors? Evidence from peer data breaches and cyber risk factors. *SSRN Electronic Journal* .
- Atasoy H, yu Chen P, Ganju K (2017) The spillover effects of health IT investments on regional healthcare costs. *Management Science* 64(6):2515–2534.
- August T, Dao D, Kim K (2019) Market Segmentation and Software Security: Pricing Patching Rights. *Management Science* 65(10):4575–4597.
- August T, Niculescu MF, Shin H (2014) Cloud implications on software network structure and security risks. *Information Systems Research* 25(3):489–510.
- August T, Tunca TI (2006) Network Software Security and User Incentives. *Management Science* 52(11):1703–1720.
- Ayabakan S, Bardhan I, Zheng Z, Kirksey K (2017) the Impact of Health Information Sharing on Duplicate Testing. *MIS Quartely* 41(4):1083–1103.
- Ayer T, Ayvaci MU, Karaca Z, Vlachy J (2019) The Impact of Health Information Exchanges on Emergency Department Length of Stay. *Production and Operations Management* 28(3):740–758.
- Baker A, Larcker DF, Wang CCY (2021) How Much Should We Trust Staggered Difference-In-Differences Estimates? *SSRN Electronic Journal* (March).
- Bakos JY (1991) Information Links and Electronic Marketplaces : The Role of Interorganizational Information Systems in Vertical Markets. *Journal of Management Information Systems* 8(2):31–52.

- Bana S, Brynjolfsson E, Jin W, Steffen S, Wang X (2021) Cybersecurity Hiring in Response to Data Breaches. *SSRN Electronic Journal* 1–30.
- Barber B, Lehavy R, McNichols M, Trueman B (2001) Can Investors Profit from the Prophets ? Security Analyst Recommendations and Stock Returns. *The Journal of Finance* 56(2):531–563.
- Barillon T (2019) Comprehensive Vulnerability Management in Connected Security Solutions. Available at <https://securityintelligence.com/comprehensive-vulnerability-management-in-connected-security-solutions/>.
- Baskerville R, Rowe F, Wolff FC (2018) Integration of Information Systems and Cybersecurity Countermeasures. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems* 49(1):33–52.
- Becker GS (1968) Crime and Punishment : An Economic Approach. *Journal of Political Economy* 76(2):169–217.
- Beyer A, Cohen DA, Lys TZ, Walther BR (2010) The financial reporting environment: Review of the recent literature. *Journal of Accounting and Economics* 50(2-3):296–343.
- Bharadwaj AS (2000) A resource-based perspective on information technology capability and firm performance: An empirical investigation. *MIS Quarterly* 24(1):169–193.
- Bisson D (2017) Should Security Researchers Protect Organizations by Any Means Necessary? Available at <https://www.tripwire.com/state-of-security/security-data-protection/security-researchers-protect-organizations-means-necessary/>.
- Blizard D (2020) Cybersecurity Operations: 5 Ways to Cut Costs Without Pain. Available at <https://securityintelligence.com/posts/cybersecurity-budget-savings/>.
- Bloomberg J (2018) To Patch or Not To Patch? Surprisingly, That Is the Question. Available at <https://www.forbes.com/sites/jasonbloomberg/2018/04/16/to-patch-or-not-to-patch-surprisingly-that-is-the-question/?sh=4545556b58fe>.
- Boudreau KJ, Lacetera N, Lakhani KR (2011) Incentives and Problem Uncertainty in Innovation Contests: An Empirical Analysis. *Management Science* 57(5):843–863.
- Boudreau KJ, Lakhani KR, Menietti M (2016) Performance responses to competition across skill levels in rank-order tournaments: Field evidence and implications for tournament design. *RAND Journal of Economics* 47(1):140–165.
- Bracken B (2021) How to Get into the Bug-Bounty Biz: The Good, Bad and Ugly. Available at <https://threatpost.com/how-to-bug-bounties/165657/>.
- Broshevan E (2019) Why Every Organization Needs a Bug Bounty Program. Available at <https://techbeacon.com/security/why-every-organization-needs-bug-bounty-program>.
- Brown J, Minor DB (2014) Selecting the Best? Spillover and Shadows in Elimination Tournaments. *Management Science* 60(12):3087–3102.

Brown SV, Tucker JW (2011) Large-Sample Evidence on Firm's Year-over-Year MDA Modifications. *Journal of Accounting Research* 49(2):309–346.

Bugcrowd (2015) This is Why Companies are Afraid of Bug Bounties. Available at <https://forum.bugcrowd.com/t/this-is-why-companies-are-afraid-of-bug-bounties/813>.

Bugcrowd (2017) Getting Started – Bug Bounty Hunter Methodology. Available at <https://www.bugcrowd.com/blog/getting-started-bug-bounty-hunter-methodology/>.

Bugcrowd (2021) Illustrated Guide to Bug Bounties Step #1: Planning. Available at <https://www.bugcrowd.com/blog/illustrated-guide-to-bug-bounties-step-1-planning/>.

Burde H (2011) The HITECH Act: An Overview. accessed on 2020-12-11.

Business Wire (2020) 2020 IT Spending: Cybersecurity Remains an Investment Priority Despite Overall IT Budget Cuts, Kaspersky Found. Available at <https://www.businesswire.com/news/home/20200930005611/en/>.

Callaway B, Sant'Anna PH (2020) Difference-in-Differences with multiple time periods. *Journal of Econometrics* 1–45.

Cao SS, Fang VW, (Gillian) Lei L (2021) Negative Peer Disclosure. *Journal of Financial Economics* 140(3):815–837.

Cassin H (2020) Are 'Bug Bounties' the Next Big Thing for Compliance? Available at <https://fcpablog.com/2020/09/28/are-bug-bounties-the-next-big-thing-for-compliance/>.

Cavalancia N (2020) Vulnerability Management Explained. Available at <https://cybersecurity.att.com/blogs/security-essentials/vulnerability-management-explained>.

Cavusoglu H, Cavusoglu H, Raghunathan S (2007) Efficiency of Vulnerability Disclosure Mechanisms to Disseminate Vulnerability Knowledge. *IEEE Transactions on Software Engineering* 33(3):171–185.

Cavusoglu H, Cavusoglu H, Zhang J (2008) Security Patch Management: Share the Burden or Share the Damage? *Management Science* 54(4):657–670.

Cazier RA, McMullin JL, Treu JS (2021) Are Lengthy and Boilerplate Risk Factor Disclosures Inadequate? An Examination of Judicial and Regulatory Assessments of Risk Factor Language. *The Accounting Review* 96(4):131–155.

Cezar A, Cavusoglu H, Raghunathan S (2014) Outsourcing Information Security: Contracting Issues and Security Implications. *Management Science* 60(3):638–657.

Chan J, Ghose A (2014) Internet's Dirty Secret: Assessing The Impact Of Online Intermediaries on HIV Transmission. *MIS Quarterly* 38(4):955–975.

Chatterjee D, TRavichandran (2013) Governance of Interorganizational Information Systems : A Resource Dependence Perspective. *Information Systems Research* 24(March 2014):261–278.

Chen, Kataria, Krishnan (2011) Correlated Failures, Diversification, and Information Security Risk Management. *MIS Quarterly* 35(2):397–422.

Cheng Z, Rai A, Tian F, Xu SX (2021) Social learning in information technology investment: The role of board interlocks. *Management Science* 67(1):547–576.

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

Choi SJ, Johnson EM (2019) Understanding the relationship between data breaches and hospital advertising expenditures. *American Journal of Managed Care* 25(1):E14–E20.

Cimpanu C (2020) Zoom to Revamp Bug Bounty Program, Bring in More Security Experts. Available at <https://www.zdnet.com/article/zoom-to-revamp-bug-bounty-program-bring-in-more-security-experts/>.

Cinelli C, Forney A, Pearl J (2020) A Crash Course in Good and Bad Controls. *SSRN Electronic Journal* 1–27.

Cohen WM, Levinthal DA (1990) Absorptive Capacity : A New Perspective on Learning and Innovation. *Administrative Science Quarterly* 35(1):128–152.

Combs V (2022) Credit agency warns weak cybersecurity defenses could hurt a company's credit rating, even before an attack. Available at <https://www.techrepublic.com/article/credit-agency-warns-weak-cybersecurity-defenses-could-hurt-a-companys-credit-rating-even-before-an-attack/>.

Comeau Z (2021) Report: Remote Work Makes Patch Management Much Harder. Available at <https://mytechdecisions.com/it-infrastructure/report-remote-work-makes-patch-management-much-harder/>.

Crews P, Kuszmaul W, Penkov P (2018) To Disclose or not Disclose: The Ethics of Vulnerability Disclosure. Available at <https://medium.com/@ptcrews/to-disclose-or-not-disclose-the-ethics-of-vulnerability-disclosure-aaf09c1ab4b0>.

D'Arcy J, Idris A, Angst CM, Hall P (2020) Too Good to Be True : Firm Social Performance and the Risk of Data Breach Too Good to Be True : Firm Social Performance and the Risk of Data Breach. *Information Systems Research* 1–45.

Dawes SS (1996) Interagency Information Sharing : Expected Benefits , Monogeeble Risks 15(3):377–394.

Dehejia RH, Wahba S (2002) Propensity score-matching methods for nonexperimental causal studies. *Review of Economics and Statistics* 84(1):151–161.

Demirezen EM, Kumar S, Sen A (2016) Sustainability of Healthcare Information Exchanges : A Game-Theoretic Approach. *Information Systems Research* 27(2):240–258.

Dempsey K, Chawla NS, Johnson A, Johnson R, Jones AC, Orebaugh A, Scholl M, Stine K (2012) Information Security. *NIST Special Publication* .

Department of Justice (2022) Department of Justice Announces New Policy for Charging Cases under the Computer Fraud and Abuse Act. Available at <https://www.justice.gov/opa/pr/department-justice-announces-new-policy-charging-cases-under-computer-fraud-and-abuse-act>.

Derouiche I, Manita R, Muessig A (2021) *Risk disclosure and firm operational efficiency*, volume 297 (Springer US).

Dey D, Lahiri A, Zhang G (2014) Quality competition in the security software market. *Management Information Systems Quarterly* 38(2):589–6060.

Diamond DW (1985) Optimal Release of Information By Firms. *The Journal of Finance* 40(4):1071–1094.

Dignan L (2014) Target CIO Jacob resigns following data breach. Available at <https://www.zdnet.com/article/are-you-ready-for-the-worst-economy-class-airline-seats-in-the-world/>.

Diosi D (2022) How to secure hotel business communications against data breaches? Available at <https://www.hospitalitynet.org/opinion/4109856.html>.

DiPalantino D, Vojnovic M (2009) Crowdsourcing and All-pay Auctions. *Proceedings of the Tenth ACM Conference on Electronic Commerce - EC '09* 119.

Dobkin C, Finkelstein A, Kluender R, Notowidigdo MJ (2018) The Economic Consequences of Hospital Admissions. *American Economic Review* 108(2):308–352.

Eastwood B (2021) It's time to bridge the gap between security and development. Available at <https://www.cybersecuritydive.com/news/security-development-devsecops/604636/>.

Elazari A (2018) The Law and Economics of Bug Bounties .

Ellis C (2021) NIST: Vulnerability Disclosure as A Requirement for Every Organization. Available at <https://www.bugcrowd.com/blog/nist-vulnerability-disclosure-as-a-requirement-for-every-organization/>.

Esmailzadeh P, Mirzaei T (2019) The potential of blockchain technology for health information exchange: Experimental study from patients' perspectives. *Journal of Medical Internet Research* 21(6)::e14184.

Everson J, Adler-Milstein J (2016) Engagement in hospital health information exchange is associated with vendor marketplace dominance. *Health Affairs* 35(7):1286–1293.

Fang F, Parameswaran M, Zhao X, Whinston AB (2014) An economic mechanism to manage operational security risks for inter-organizational information systems. *Information Systems Frontiers* 16(3):399–416.

Feldman SS, Schooley BL, Bhavsar GP (2014) Health information exchange implementation: Lessons learned and critical success factors from a case study. *Journal of Medical Internet Research* 16(8):e19.

Financial Times (2014) Cyber security: first mover disadvantage. Available at <https://www.ft.com/content/803ea71e-3948-11e4-9cce-00144feabdc0>.

- Finifter M, Akhawe D, Wagner D (2013) An Empirical Study of Vulnerability Rewards Programs. *Proceedings of the 22Nd USENIX Conference on Security* 273–288.
- Fischer T, Huber T, Dibbern J, Hirschheim R (2012) The Evolution of Contractual and Relational Governance in IS Outsourcing.
- Florakis C, Louca C, Michaely R, Weber M (2020) Cybersecurity Risk. *SSRN Electronic Journal* .
- Foerderer J, Schuetz SW (2022) Data Breach Announcements and Stock Market Reactions: A Matter of Timing? *Management Science* (February).
- Forman C, van Zeebroeck N (2012) From Wires to Partners: How the Internet Has Fostered RD Collaborations Within Firms. *Management Science* 58(8):1549–1568.
- Francis J, Nanda D, Wang X (2006) Re-examining the effects of regulation fair disclosure using foreign listed firms to control for concurrent shocks. *Journal of Accounting and Economics* 41(3):271–292.
- Frenkel S, Guttman I, Kremer I (2020) The effect of exogenous information on voluntary disclosure and market quality. *Journal of Financial Economics* 138(1):176–192.
- Fruhlinger J (2020) Top Cybersecurity Facts, Figures and Statistics for 2020. Available at <https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html>.
- Fryer H, Simperl E (2017) Web Science Challenges in Researching Bug Bounties. *Proceedings of the 2017 ACM on Web Science Conference - WebSci '17*, 273–277.
- Gal-Or E, Chose A (2005) The Economic Incentives for Sharing Security Information. *Information Systems Research* 16(2):186–208.
- Gamero-Garrido A, Savage S, Levchenko K, Snoeren AC (2017) Quantifying the Pressure of Legal Risks on Third-party Vulnerability Research. *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security - CCS '17*, 1501–1513.
- Gasparas J, Monteiro E (2009) Cross-contextual use of integrated information systems. *ECIS 2009 Proceedings*.
- Gaynor MS, Hydari MZ, Telang R (2012) Is Patient Data Better Protected in Competitive Healthcare Markets? *WEIS (Weis)*:1–27.
- Geng XGX, Whinston AB (2000) Defeating distributed denial of service attacks.
- Giboney JS, Proudfoot JG, Goel S, Valacich JS (2016) The Security Expertise Assessment Measure (SEAM): Developing a Scale for Hacker Expertise. *Computers and Security* 60:37–51.
- Gil-Garcia JR, Sayogo DS (2016) Government inter-organizational information sharing initiatives: Understanding the main determinants of success. *Government Information Quarterly* 33(3):572–582.
- Goodman-Bacon A (2021) Difference-in-differences with variation in treatment timing. *Journal of Econometrics* .

Gordon LA, Loeb MP (2002) The Economics of Information Security Investment. *ACM Transactions on Information and System Security* 5(4):438–457.

Gordon LA, Loeb MP, Sohail T (2010) Market value of voluntary disclosures concerning information security. *MIS Quarterly* 34(3):567–594.

Greenwood BN, Wattal S (2017) Show Me the Way to Go Home: An Empirical Investigation of Ride-Sharing and Alcohol Related Motor Vehicle Fatalities. *MIS Quarterly* 41(1):163–187.

Greig J (2022) Data breach: Broward Health warns 1.3 million patients, staff of 'medical identity theft'. Available at <https://www.zdnet.com/article/broward-health-warns-1-3-million-patients-staff-of-medical-identity-theft-after-data-breach/>.

Grover V, Kohli R (2012) Cocreating IT value: New capabilities and metrics for multifirm environments. *MIS Quarterly* 36(1):225–232.

Hackerone (2019) The Beginners' Guide to Bug Bounty Programs. Available at <https://www.hackerone.com/resources/e-book/the-beginners-guide-to-bug-bounty-programs-1>.

Hamre GA, Monteiro E (2013) Towards a socio-technically resilient collaborative medication process. *CEUR Workshop Proceedings* 984(1):1–9.

Harrington T (2021) Why a skills shortage is one of the biggest security challenges for companies. Available at <https://resources.infosecinstitute.com/topic/why-a-skills-shortage-is-one-of-the-biggest-security-challenges-for-companies/>.

Hata H, Guo M, Babar MA (2017) Understanding the Heterogeneity of Contributors in Bug Bounty Programs. *International Symposium on Empirical Software Engineering and Measurement*, volume 2017, 223–228.

Havakhor T, Rahman MS, Zhang T (2020) Cybersecurity Investments and the Cost of Capital. *SSRN Electronic Journal* 1–48.

Haworth J (2021) When vulnerability disclosure goes sour: New GitHub repo details legal threats and risks faced by ethical hackers. Available at <https://portswigger.net/daily-swig/when-vulnerability-disclosure-goes-sour-github-repo-details-legal-threats-and-risks-faced-by-ethical-hackers>.

Haynes A, Sadeghipour B (2021) Crowdsourced Bug Bounty Programs: Security Gains Versus Potential Losses. Available at <https://www.infosecurity-magazine.com/magazine-features/crowdsourced-bug-bounty-programs/>.

He S, Rui H, Whinston AB (2018) Social media strategies in product harm crises. *Information Systems Research* 29(2):362–3.

Healy PM, Palepu KG (2001) Information asymmetry, corporate disclosure and the capital markets: A review of the empirical disclosure literature. *Journal of Accounting and Economics* 31(1-3):405–440.

Heinle MS, Smith KC (2017) A theory of risk disclosure. *Review of Accounting Studies* 22(4):1459–1491.

Help Net Security (2019) Week in Review: Worst Passwords of 2019, the End of Windows 7, 2020 Cybersecurity Trends. Available at <https://www.helpnetsecurity.com/2019/12/22/week-in-review-worst-passwords-of-2019-the-end-of-windows-7-2020-cybersecurity-trends/>.

HHS (2015) The HIPAA Privacy Rule and Electronic Health Information Exchange in a Networked Environment. Technical report.

Hilary G, Segal B, Zhang MH (2016) Cyber-Risk Disclosure : Who Cares ?

Hoberg G, Phillips G (2016) Text-based network industries and endogenous product differentiation. *Journal of Political Economy* 124(5):1423–1465.

Hoffman S, Podgurski A (2009) Scholarly Commons E-Health Hazards: Provider Liability and Electronic Health Record Systems E-HEALTH HAZARDS: PROVIDER LIABILITY AND ELECTRONIC HEALTH RECORD SYSTEMS. *Scholarly Commons* .

Hsu C, Lee JN, Straub DW (2012) Institutional influences on information systems security innovations. *Information Systems Research* .

Hu M, Wang L (2021) Joint vs. Separate Crowdsourcing Contests. *Management Science* 67(5):2711–2728.

Huang CD, Behara RS, Goo J (2014) Optimal information security investment in a Healthcare Information Exchange: An economic analysis. *Decision Support Systems* .

Hui KL, Hui W, Yue WT (2012) Information Security Outsourcing with System Interdependency and Mandatory Security Requirement. *Journal of Management Information Systems* 29(3):117–156.

Hui KL, Ke PF, Yao Y, Yue WT (2019) Bilateral Liability-based Contracts in Information Security Outsourcing. *Information Systems Research* 30(2):411–429.

Hui KL, Kim SH, Wang QH (2017) Cybercrime Deterrence and International Legislation: Evidence From Distributed Denial of Service Attacks. *MIS Quarterly* 41(2):497–A11.

Iacus SM, King G, Porro G (2012) Causal inference without balance checking: Coarsened exact matching. *Political Analysis* 20(1):1–24.

IBM (2021) IBM Report: Cost of a Data Breach Hits Record High During Pandemic. Available at <https://newsroom.ibm.com/2021-07-28-IBM-Report-Cost-of-a-Data-Breach-Hits-Record-High-During-Pandemic>.

Iyengar R (2020) Massive SolarWinds hack has big businesses on high alert. Available at <https://www.cnn.com/2020/12/19/tech/solarwinds-hack-companies/index.html>.

Janakiraman R, Lim JH, Rishika R (2018) The Effect of a Data Breach Announcement on Customer Behavior: Evidence from a Multichannel Retailer. *Journal of Marketing* 82(2):85–105.

Ji YH, Kumar S, Mookerjee V (2016) When Being Hot Is Not Cool: Monitoring Hot Lists for Information Security. *Information Systems Research* 27(4):897–918.

JMPorup (2018) Bug bounties offer legal safe harbor. Right? Right? Available at <https://www.csoonline.com/article/3295860/bug-bounties-offer-legal-safe-harbor-right-right.html>.

Kaczanowski M (2020) What is a Bug Bounty Program? How Bug Bounties Work and Who Should Use Them.

Kamiya S, Kang JK, Kim J, Milidonis A, Stulz RM (2021) Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics* 139(3):719–749.

Kannan K, Rahman MS, Tawarmalani M (2016) Economic and Policy Implications of Restricted Patch Distribution. *Management Science* 62(11):3161–3182.

Kannan K, Telang R (2005) Market for Software Vulnerabilities? Think Again. *Management Science* 51(5):726–740.

Kelton AS, Pennington RR (2020) Do voluntary disclosures mitigate the cybersecurity breach contagion effect? *Journal of Information Systems* 34(3):133–157.

Kerner SM (2019) Why Hyatt Is Launching a Public Bug Bounty Program. Available at <https://www.eweek.com/security/why-hyatt-is-launching-a-public-bug-bounty-program/>.

Kim SH, Kwon J (2019) How Do EHRs and a Meaningful Use Initiative Affect Breaches of Patient Information? *Information Systems Research* (September).

King G, Nielsen R (2019) Why Propensity Scores Should Not Be Used for Matching. *Political Analysis* 27(4):435–454.

Kleis L, Chwelos P, Ramirez RV, Cockburn I (2012) Information technology and intangible output: The impact of IT investment on innovation productivity. *Information Systems Research* 23(1):42–59.

Körpeoğlu E, Cho SH (2018) Incentives in Contests with Heterogeneous Solvers. *Management Science* 64(6):2709–2715.

Krieger JL (2021) Trials and Terminations: Learning from Competitors' RD Failures. *Management Science* (July).

Kumar K, Dissel HGV (1996) Sustainable Collaboration: Managing Conflict and Cooperation in Interorganizational Systems. *Management Information Systems Quarterly* 20(3):279–300.

Kunreuther H, Heal G (2003) Interdependent Security. *Journal of Risk and Uncertainty* 26(2-3):231–249.

Kwon J, Johnson M (2018) Meaningful healthcare security: Does meaningful-use attestation improve information security performance? *MIS Quarterly* 42(4):1043–1067.

Kwon J, Johnson ME (2014) Proactive Versus Reactive Security Investments in the Healthcare Sector. *MIS Quarterly* 38(2):451–471.

Lambert R, Leuz C, Verrecchia RE (2007) Accounting information, disclosure, and the cost of capital. *Journal of Accounting Research* 45(2):385–420.

- Larson A (1992) Network Dyads in Entrepreneurial Settings: A Study of the Governance of Exchange Relationships. *Administrative Science Quarterly* 37(1):76.
- Laszka A, Zhao M, Malbari A, Grossklags J (2018) The Rules of Engagement for Bug Bounty Programs. *International Conference on Financial Cryptography and Data Security*, 138–159 (Berlin, Heidelberg: Springer).
- Lee CH, Geng X, Raghunathan S (2013) Contracting Information Security in the Presence of Double Moral Hazard. *Information systems research* 24(2):295–311.
- Lee CH, Geng X, Raghunathan S (2016) Mandatory standards and organizational information security. *Information Systems Research* 27(1):70–86.
- Lemos R (2021) Bug Bounties Surge as Firms Compete for Talent. Available at <https://www.darkreading.com/application-security/bug-bounties-surge-as-firms-compete-for-talent>.
- Liu CW, Huang P, Lucas HC (2020) Centralized IT Decision Making and Cybersecurity Breaches: Evidence from U.S. Higher Education Institutions. *Journal of Management Information Systems* 37(3):758–787.
- Lynch K (2021) Supreme Court Offers Justice for Cybersecurity Threat Hunters Options. Available at <https://www.mimecast.com/blog/supreme-court-offers-justice-for-cybersecurity-threat-hunters/>.
- Malladi SS, Subramanian H (2019) Bug Bounty Programs for Cybersecurity: Practices, Issues, and Recommendations. *IEEE Software* 37(1):31–39.
- Malone TW (1987) Modeling Coordination in Organizations and Markets. *Management Science* 33(10):1317–1332.
- Marino A (2020) How the Commercialization of Bug Bounties is Creating More Vulnerabilities. Available at <https://bit.ly/3pxQDJb>.
- Marks J (2018) Congress Has Gone Bananas for Bug Bounties, but They May Not Always Be the Right Choice. Available at <https://bit.ly/3pvZb3t>.
- Martin KD, Borah A, Palmatier RW (2017) Data Privacy: Effects on Customer and Firm Performance. *Journal of Marketing* 81(1):36–58.
- McGee MK (2016) Clinic Reports Security Incident Involving HIE Access. Available at <https://www.careersinfosecurity.com/clinic-reports-security-incident-involving-hie-access-a-9413>.
- McGowan JJ, Kuperman GJ, Olinger L, Russell C (2012) Strengthening health information exchange. Technical Report 301.
- Miller AR, Tucker C (2009) Privacy Protection and Technology Diffusion: The Case of Electronic Medical Records (Electronic Companion). *Management Science* 55(7).
- Miller AR, Tucker C (2014) Health information exchange, system size and information silos. *Journal of Health Economics* 33(1):28–42.
- Miller AR, Tucker CE (2011) Encryption and the loss of patient data. *Journal of policy analysis and management : [the journal of the Association for Public Policy Analysis and Management]* 30(3):534–556.

Mitra S, Ransbotham S (2015) Information Disclosure and the Diffusion of Information Security Attacks. *Information Systems Research* 26(3):565–584.

Mo J, Sarkar S, Chen J (2019) Sponsored Tasks and Solver Participation in Crowdsourcing Contests. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3388758.

Moldovanu B, Sela A (2001) The Optimal Allocation of Prizes in Contests. *American Economic Review* 91(3):542–558.

Monica K (2018) 70 % of Hospitals participated in nationwide HIE networks in 2017. Available at <https://ehrintelligence.com/news/70-of-hospitals-participated-in-nationwide-hie-networks-in-2017>.

Mont J (2015) Why Boilerplate Battles Continue to Rage. Available at <https://www.complianceweek.com/why-boilerplate-battles-continue-to-rage/3393.article>.

Moore T (2010) Introducing the Economics of Cybersecurity : Principles and Policy Options. *Proceedings of a Workshop on Deterring Cyberattacks* (National Academies Press).

Morgan S (2019) Global Cybersecurity Spending Predicted to Exceed \$1 Trillion From 2017-2021. Available at <https://cybersecurityventures.com/cybersecurity-market-report/>.

NCSL (2021) Security Breach Notification Laws. Available at <https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx>.

Neumann J, Hudson D (2021) Beware the Bug Bounty. Available at <https://www.darkreading.com/vulnerabilities---threats/beware-the-bug-bounty/a/d-id/1340658>.

Newman D (2017) Complex and Fragmented Systems are the Enemy to Security. Available at <https://futurumresearch.com/complex-fragmented-systems-enemy-security/>.

Nidecki TA (2020) 7 Steps to Avoid Uncoordinated Vulnerability Disclosure. Available at <https://www.acunetix.com/blog/web-security-zone/7-steps-avoid-uncoordinated-vulnerability-disclosure/>.

Nieuwesteeg B, Faure M (2018) An analysis of the effectiveness of the EU data breach notification obligation. *Computer Law and Security Review* 34(6):1232–1246.

NIST (2010) Security architecture design process for health information exchanges (HIEs). Technical report.

NIST (2014) Framework for improving critical infrastructure cybersecurity: Version 1.0. Technical report.

NIST (2018) Framework for Improving Critical Infrastructure Cybersecurity. Technical report.

Novet J (2020) SolarWinds hack has shaved 23% this week, Available at <https://www.cnbc.com/2020/12/16/solarwinds-hack-triggers-23percent-stock-haircut-this-week-so-far.html>.

- Ogut HU, Menon N, Ragnathan S (2004) Cyber Insurance and IT Security Investment: Impact of Interdependent Risk. *Infoecon.Net* 1–30.
- Osborne C (2018) Disclose.io: A safe harbor for hackers disclosing security vulnerabilities. Available at <https://www.zdnet.com/article/disclose-io-a-safe-harbor-for-hackers-involved-in-vulnerability-disclosure/>.
- Osborne C (2022) Zoom awarded \$1.8 million in bug bounty rewards over 2021. Available at <https://www.zdnet.com/article/zoom-awards-1-8-million-in-bug-bounty-rewards-over-2021/>.
- Owens C (2018) Low Hanging Fruit Often Abused by Red Teams. Available at <https://bit.ly/3irIogy>.
- Pan Y, Huang P, Gopal A (2019) Storm Clouds on the Horizon? New Entry Threats and RD Investments in the U.S. IT Industry. *Information Systems Research* 30(2):540–562.
- Pang MS, Tanriverdi H (2022) Strategic roles of IT modernization and cloud migration in reducing cybersecurity risks of organizations: The case of U.S. federal government. *Journal of Strategic Information Systems* 31(1):101707.
- Park J, Sani J, Shroff N, White H (2019) Disclosure incentives when competing firms have common ownership. *Journal of Accounting and Economics* 67(2-3):387–415.
- Park S, Albert K (2020) A Researcher ' s Guide to Some Legal Risks of Security Research .
- Perlroth N (2011) Digital Data on Patients Raises Risk of Breaches. Available at <https://www.nytimes.com/2011/12/19/technology/as-patient-records-are-digitized-data-breaches-are-on-the-rise.html>.
- Petersen C (2019) A CTO's Take on the Security Operations Maturity Model. Available at <https://bit.ly/3v5U37f>.
- Pfefferkorn R (2020) The Importance of Protecting Good-faith Security Research. Available at <http://cyberlaw.stanford.edu/blog/2020/09/importance-protecting-good-faith-security-research>.
- Poppo L, Zenger T (2002) Do formal contracts and relational governance function as substitutes or complements? *Strategic Management Journal* 23(8):707–725.
- Pratt MK (2022) 12 steps to building a top-notch vulnerability management program. Available at <https://www.csoonline.com/article/3659838/12-steps-to-building-a-top-notch-vulnerability-management-program.html>.
- Ransbotham S, Mitra S (2009) Choice and chance: A conceptual model of paths to information security compromise. *Information Systems Research* 20(1):121–139.
- Ransbotham S, Ramsey J (2012) Are Markets for Vulnerabilities Effective. *MIS Quarterly* 36(1):43–64.
- Raymond E (1999) The Cathedral and the Bazaar. *Knowledge, Technology & Policy* 12(3):23–49.
- Roberts N, Galluch PS, Din M, Grover V (2012) Absorptive Capacity and Information Systems Research: Review, Synthesis, And Directions for Future Research. *MIS Quarterly* 36(2):625–648.

Robey D, Im G, Wareham JD (2008) Theoretical Foundations of Empirical Research on Interorganizational Systems: Assessing Past Contributions and Guiding Future Directions. Technical Report 9.

Robinson RM (2017) Back to Basics: Six Simple Strategies to Strengthen Your Security Posture. Available at <https://securityintelligence.com/back-to-basics-six-simple-strategies-to-strengthen-your-security-posture/>.

Rogers JL, Schrand CM, Zechman SLC (2014) Do Managers Tacitly Collude to Withhold Industry-Wide Bad News? *SSRN Electronic Journal* (13).

Romanosky S, Telang R, Acquisti A (2011) Do Data Breach Disclosure Laws Reduce Identity Theft. *Journal of Policy Analysis and Management* 32(2):296–322.

Ross SE, Schilling LM, Fernald DH, Davidson AJ, West DR (2010) Health information exchange in small-to-medium sized family medicine practices: Motivators, barriers, and potential facilitators of adoption. *International Journal of Medical Informatics* 79(2):123–129.

Rudin RS, Motala A, Goldzweig CL, Shekelle PG (2014) Usage and effect of health information exchange: A systematic review. *Annals of Internal Medicine* 161(11):803–811.

Sarkar S, Vance A, Ramesh B, Demestihis M, Wu DT (2020) The influence of professional subculture on information security policy violations: A field study in a healthcare context. *Information Systems Research* 31(4):1240–1259.

Schechter S (2002) How to Buy Better Testing Using Competition to Get the Most Security and Robustness for Your Dollar. *International Conference on Infrastructure Security*, 73–87.

Schmit CD, Wetter SA, Kash BA (2017) Falling short: how state laws can address health information exchange barriers and enablers. *Journal of the American Medical Informatics Association* 0(April):1–11.

Schneier B (2007) Schneier: Full Disclosure of Security Vulnerabilities a 'Damned Good Idea'. Available at https://www.schneier.com/essays/archives/2007/01/schneier_full_disclo.html, accessed on 2021-09-26.

SEC (2011) CF Disclosure Guidance: Topic No.2 Cybersecurity. Available at <https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm>.

SEC (2022) SEC Proposes Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies. Available at <https://www.sec.gov/news/press-release/2022-39>.

Seh AH, Zarour M, Alenezi M, Sarkar AK, Agrawal A, Kumar R, Ahmad Khan R (2020) Healthcare Data Breaches: Insights and Implications. *Healthcare* 8(2):133.

Sen R, Choobineh J, Kumar S (2019) Determinants of Software Vulnerability Disclosure Timing. *Production and Operations Management* 0(0):1–21.

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

- Shein E (2022) Small and midsize businesses can mitigate security risks with patch management. Available at <https://www.computerworld.com/article/3651450/small-and-midsize-businesses-can-mitigate-security-risks-with-patch-management.html>.
- Shrobe H, Shrier DL, Pentland A (2018) *New Solutions for Cybersecurity* (MIT Press).
- Siponen M, Vance A (2010) Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly* 34(SPEC. ISSUE 3):487–502.
- Sittig DF, Singh H (2011) Legal, Ethical, and Financial Dilemmas in Electronic Health Record Adoption and Use. *Pediatrics* 127(4):e1042–e1047.
- Skinner DJ (1994) Why Firms Voluntarily Disclose Bad News. *Journal of Accounting Research* 32(1):38–60.
- Snell E (2015) How to Improve Health Data Privacy, Security in HIE. Available at <https://healthitsecurity.com/news/how-to-improve-health-data-privacy-security-in-hie>, accessed on 2020-12-11.
- Souppaya M, Scarfone K (2022) Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology. Technical report.
- Sridhar K, Ng M (2021) Hacking for Good: Leveraging HackerOne Data to Develop an Economic Model of Bug Bounties. *Journal of Cybersecurity* 7(1):1–9.
- Staiger BYD, Stock JH (1997) Instrumental Variables Regression with Weak Instruments. *Econometrica* 65(3):557–586.
- Statista (2021) Industry Share of Bug Bounty Programs Worldwide in 2020. Available at <https://www.statista.com/statistics/1051970/worldwide-bug-bounty-program-industry/>.
- Storm D (2015) United Airlines waits 6 months to patch critical flaw submitted to bug bounty program. Available at <https://www.computerworld.com/article/3007305/united-airlines-waits-6-months-to-patch-critical-flaw-submitted-to-bug-bounty-program.html>.
- Stouras KI, Hutchison-Krupat J, Chao RO (2021) The Role of Participation in Innovation Contests. *Management Science* (February 2022).
- Straub DW, Nance WD (1990) Discovering and Disciplining Computer Abuse in Organizations: A Field Study. *MIS Quarterly* 14(1):45.
- Sun S, Lu SF, Rui H (2020) Does telemedicine reduce emergency room congestion? evidence from new york state. *Information Systems Research* 31(3):972–986.
- Tanimura JK, Wehrly EW (2015) The market value and reputational effects from lost confidential information. *International Journal of Financial Management* 5(4).
- Tanriverdi H, Roumani Y, KNwankpa J (2019) Structural Complexity and Data Breach Risk. 1–17 (ICIS2019).
- Telang R, Wattal S (2007) An empirical analysis of the impact of software vulnerability announcements on firm stock price. *IEEE Transactions on Software Engineering* 33(8):544–557.

Teoh SH, Hwang CY (1991) Nondisclosure and Adverse Disclosure as Signals of Firm Value 4(2):283–313.

Terrill C (2018) Is Your Company Ready For A Bug Bounty Program? Available at <https://www.forbes.com/sites/christieterrill/2018/09/05/is-your-company-ready-for-a-bug-bounty-program/?sh=507d2da15204>.

Terwiesch C, Xu Y (2008) Innovation Contests, Open Innovation, and Multiagent Problem Solving. *Management Science* 54(9):1529–1543.

Turton W, Bloomberg (2020) Hackers used a little-known IT vendor to attack U.S. agencies. Available at <https://fortune.com/2020/12/15/solarwinds-hackers-u-s-agencies/>.

Ustinov N (2021) Building An In-House Solution Vs. Buying Software: Pros And Cons To Consider. Available at <https://www.forbes.com/sites/forbestechcouncil/2021/07/29/building-an-in-house-solution-vs-buying-software-pros-and-cons-to-consider/?sh=40ef7da67dc5>.

Vance A, Jenkins JL, Anderson BB, Bjornn DK, Kirwan CB (2018) Tuning out security warnings: A longitudinal examination of habituation through fMRI, eye tracking, and field experiments. *MIS Quarterly* 42(2):355–380.

Verrecchia RE (1983) Discretionary disclosure. *Journal of Accounting and Economics* 5:179–194.

Vice R (2022) Hiring In-House Developers Or An Outside Firm: Pros And Cons When Building New Software. Available at <https://www.forbes.com/sites/forbestechcouncil/2022/03/21/hiring-in-house-developers-or-an-outside-firm-pros-and-cons-when-building-new-software/?sh=4b4f2db91191>.

Votipka D, Stevens R, Redmiles E, Hu J, Mazurek M (2018) Hackers vs. Testers: A Comparison of Software Vulnerability Discovery Processes. *Proceedings - IEEE Symposium on Security and Privacy* 2018-May:374–391.

Walshe T, Simpson A (2020) An Empirical Study of Bug Bounty Programs. *IBF 2020 - Proceedings of the 2020 IEEE 2nd International Workshop on Intelligent Bug Fixing*, 35–44.

Wang ETG, Seidmann A (1995) Electronic Data Interchange: Competitive Externalities and Strategic Implementation Policies. *Management Science* 41(3):401–418.

Wang J, Gupta M, Rao HR (2015) Insider Threats in a Financial Institution: Analysis of Attack-Proneness of Information Systems Applications. *MIS Quarterly* 39(1):91–U491.

Wang T, Kannan KN, Ulmer JR (2013) The association between the disclosure and the realization of information security risk factors. *Information Systems Research* 24(2):201–218.

Whittaker Z (2018) Lawsuits threaten infosec research — just when we need it most. Available at <https://www.zdnet.com/article/chilling-effect-lawsuits-threaten-security-research-need-it-most/>.

Wolfman J, Chipman JC, Wilson AJ, Mercer ST, Pinto TY (2022) SEC proposes new public company cybersecurity disclosure rules. Available at <https://www.wilmerhale.com/en/insights/blogs/focus-on-audit-committees-accounting-and-the-law/20220310-sec-proposes-new-public-company-cybersecurity-disclosure-rules>.

Wroten B (2020) How Bug Bounty Programs Can Help Hotels' Data Security. Available at <https://bit.ly/3xb9U5M>.

Zhang M (2017) Man Finds DJI Customer Data Exposed, Gets Threat and Rejects \$30K Bounty. Available at <https://petapixel.com/2017/11/20/man-finds-dji-customer-data-exposed-gets-threat-rejects-30k-bounty/>.

Zhang S, Singh PV, Ghose A (2019) A Structural Analysis of the Role of Superstars in Crowdsourcing Contests. *Information Systems Research* 30(1):15–33.

Zhang X, Tsang A, Yue WT, Chau M (2015) The Classification of Hackers by Knowledge Exchange Behaviors. *Information Systems Frontiers* 17(6):1239–1251.

Zhao M, Laszka A, Grossklags J (2017) Devising Effective Policies for Bug-Bounty Platforms and Security Vulnerability Discovery. *Journal of Information Policy* 7(2017):372–418.

Zhao M, Laszka A, Maillart T, Grossklags J (2016) Crowdsourced Security Vulnerability Discovery: Modeling and Organizing Bug-Bounty Programs. *The HCOMP Workshop on Mathematical Foundations of Human Computation, Austin, TX, USA*.

Zhao X, Xue L, Whinston AB (2013) Managing Interdependent Information Security Risks : Cyberinsurance , Managed Security Services , and Risk Pooling Arrangements 30(1):123–152.