THREE ESSAYS ON THE ECONOMICS OF CYBERSECURITY

By

TIANJIAN ZHANG

Bachelor of Science in Mathematics
Chinese University of Hong Kong
New Territories, Hong Kong SAR
2010

Master of Science in Mathematics
Oklahoma State University
Stillwater, Oklahoma
2015

Submitted to the Faculty of the
Graduate College of the
Oklahoma State University
in partial fulfillment of
the requirements for
the Degree of
DOCTOR OF PHILOSOPHY
May, 2020

THREE ESSAYS ON THE ECONOMICS OF

CYBERSECURITY

Dissertation Approved:

Dr. David Biros

Dissertation Adviser

Dr. Gregory Eaton

Dr. Taha Havakhor

Dr. Ramesh Sharda

ACKNOWLEDGEMENTS

In my doctoral study, I owe my biggest thanks to Dr. David Biros and Dr. Taha Havakhor. Without either of them, this dissertation and my job market outcome would look very different. There are, of course, many other faculties, friends and families that are essential in this journey.

When I first met Dr. Biros during the Ph.D. program interview, I was still a nerdy math student with practically zero knowledge in information systems. Despite my completely different academic background, Dr. Biros made a bold move to recruit me. Seeing my initial struggle in the program, he had the foresight to suggest me to work on cybersecurity, which turns out to be a highly sought-after area when I entered the job market. As my advisor, he goes out of his way to support my endeavor. He is always a text away to discuss research, give me career advice and nudge me in the right direction at the right moment. There are countless instances when Dr. Biros helped me in some small or major ways. Perhaps the most heartwarming moment is when I had some car trouble before a campus interview, he showed up at 5 am to drive me to the airport at a moment's notice. One simply cannot ask for more from his adviser.

Late in my third year, I started to work closely with Taha. Under his guidance, most of my research now situates in the intersection of cybersecurity and economics of information systems, a relatively new and vibrant niche area. Taha has not only impacted the work I did, but also the way I work. His turnaround is so fast that it has also made me (slightly) faster. I have learned from Taha the ins and outs of preparing for a journal submission, how to do a good presentation, how to interact with people during interviews, etc. While he is never shy to give me the criticisms I need, he is always generous with encouragement. After my disastrous presentation of our first project together at the 2018 Big XII+ MIS Symposium, Taha gave me the encouragement I didn't

quite deserve but desperately needed. With help from him and Dr. Biros, I slowly improved from that low point. It suffices to say my last two years of the Ph.D. study is heavily shaped by Taha.

In reaching this point, I have also benefited from the wisdom of my committee members. When I first spoke with Dr. Ramesh Sharda the summer before I entered the Ph.D. program, I thought I would be working on operations research. While my interests have evolved, his high-level perspective has influenced some of my major decisions during this journey. I have known Dr. Gregory Eaton the shortest, but Greg's influence on my research has already covered and extended beyond this dissertation. Coming from a finance background, he always offers a fresh and insightful perspective.

Other faculties and students at OSU have also played important roles in this adventure. Dr. Bryan Hammer and Dr. Andy Luse introduced me to the discipline during my first seminar, while putting up with my ignorance. Dr. Rathin Sarathy is always there when I need some sharp insights or have methodology questions. Dr. Fletcher Glancy has been quietly correcting my grammar over the years and mentored me during my very first conference trip. Our department chair Dr. Rick Wilson is always on my side and has made my life much easier when I was in the market. I also benefited from the experience of Dr. Ali Amiri, Dr. Corey Baham, Dr. Obi Ogbanufe, Dr. Jim Burkman, Dr. Nik Dalal, Dr. Chenzhang Bao, Dr. Federico Aime, and Dr. Bryan Edwards. I thank my teaching coordinators Dr. Tim Ireland and Dr. Mark Weiser for their guidance. I would also like to thank my Ph.D. peers. The younger Ph.D. students in our program have pushed me to set up a decent example just like the ones before me. I want to thank my master adviser, Mahdi Asgari, who sharply spotted my weaknesses in pure mathematics, and suggested me to take on a more applied route for my Ph.D.

My parents have shaped my writing abilities and suggested me to major in economics when I wanted to become a mathematician or an astronomer. While I resisted their suggestion for years, I am now essentially working on applied economics. Apparently, they know me better than I knew myself. Finally, I want to thank my wife Chenqi for her bluntness in criticizing my research, and for standing by me during my ups and downs.

Name: Tianjian Zhang

Date of Degree: MAY, 2020

Title of Study: THREE ESSAYS ON THE ECONOMICS OF CYBERSECURITY

Major Field: Business Administration

Abstract: The rapid growth of digitization has made cybersecurity a critical area for corporations, markets, and governments. The rise in cybersecurity investments and sweeping changes in the regulatory environment raise new economic questions – related to the impacts of cybersecurity investments, innovations, and legislation – that are yet to be answered. Focusing on the limited supply of cybersecurity labor, which has fallen behind the large demand for cybersecurity, Essay 1 studies how cybersecurity labor impacts the value of major infrastructural cyber investments. Moving beyond the ways to leverage cyberinfrastructure and labor, Essay 2 sheds light on the impact of the increasing pressure to pursue development and innovation in the cybersecurity area. This essay examines the bottom-line value of a prevalent type of innovative initiatives, i.e., corporate venture capital (CVC) investment in cybersecurity startups. Essays 1 and 2 heavily focus on the value proposition of cybersecurity investments in corporations. While both essays consider the cybersecurity legislation as exogenous variations instigating further demand for cybersecurity products and innovations, Essay 3 links a widely-adopted cybersecurity law, i.e., security breach notification law (SBNL), to the broader economic demand for general IT services. Compliance costs of cybersecurity legislation raise the barrier for general digitization initiatives, thus decreasing the demand for digitization and negatively impact general IT service providers, the main suppliers of digital goods and services. A difference-in-difference study examines how passages of SBNLs impact the employment of general IT service providers. Overall, the dissertation highlights a) the importance of cybersecurity labor in leveraging cybersecurity infrastructure, b) the business value of innovation in cybersecurity as an area that is predominantly believed to be costly but not value-generating, and c) the broader economic impacts of cybersecurity legislation. In doing so, the dissertation covers a wide range of institutional entities that both shape and are impacted by the cybersecurity ecosystem.

Keywords: Cybersecurity investment, cybersecurity labor, corporate venture capital, Tobin's Q, security breach notification law, IT employment

TABLE OF CONTENTS

Chapter Page

LIST OF TABLES

Table Page

LIST OF FIGURES

Figure Page

CHAPTER I: OVERVIEW

Cybersecurity, the protection of information in bits, is essential to the digital economy. While digital technologies bring about convenience and higher productivity, the information in digitized formats is vulnerable to unauthorized access. From 2012 to 2018, the number of data breaches in the U.S. has doubled (Sen 2018). In the meantime, all fifty states in the U.S. passed security breach notification laws (SBNLs), which require organizations to publicly disclose data breaches. The rise in cyber threats and a more stringent regulatory environment coincide with a sharp increase in cybersecurity spending (Sen 2018). The dramatic changes in the cybersecurity landscape raise new economic questions beyond those in the existing cybersecurity literature. This three-essay dissertation addresses some of these questions related to cybersecurity investments, innovations, and legislation.

Prior studies in cybersecurity have documented how various risk-mitigation mechanisms reduce risks on personal- (Bulgurcu et al. 2010; D'Arcy et al. 2009), organizational- (Angst et al. 2017; Kwon and Johnson 2018), and macro-levels (Hui et al. 2017; Romanosky et al. 2011). On the economics side, empirical studies evaluate the stock market reactions toward data breaches (Cavusoglu et al. 2004; Gordon et al. 2011), as well as the business values of cybersecurity investments (Bose and Leung 2019; Gordon et al. 2010). Despite the growing literature, existing studies have not considered cybersecurity labor or innovations and instead have focused on commoditized cyber products and services. In addition, the broader economic impacts of cybersecurity legislation are largely unknown. We attempt to fill these voids in the three essays.

Although cybersecurity investments create positive business values (Bose and Leung 2019; Chai et al. 2011; Gordon et al. 2010), the value generation mechanism and determinants of value heterogeneity are not clear. Since substantive cybersecurity investments are more effective in mitigating threats than symbolic adoptions (Angst et al. 2017) and recruitment of talents is a strong indicator of substantive initiatives, cybersecurity labor will play an important role in leveraging cybersecurity investments. The severe shortages of cybersecurity labor (Zadelhoff 2017) add to the criticalness of cybersecurity labor. Essay 1 therefore examines how cybersecurity labor impacts the value of cybersecurity investments (RQ1).

Related to labor, cybersecurity innovation is also an area under dramatic change. At the forefront of cyber innovation, cybersecurity startups are among the most vibrant entrepreneurship, with venture capital (VC) funding in cybersecurity increasing at an astonishing rate (Peterson 2018). Essay 2 focuses on a specific type of VC, corporate venture capitals (CVCs), which refer to minority equity investments made by established firms in entrepreneurial ventures. CVCs are innovation-oriented, where the investing firms learn from the startups (Ma 2019). Essay 2 determines how CVC investment in cybersecurity affects the value of the investing firm (RQ2).

Essay 3 tackles a broader agenda and addresses the economic impacts of cybersecurity legislation toward general IT. While digitization necessitates cybersecurity reforms, firms engaging in digitization initiatives may be discouraged by the costs of such major changes. Therefore, it has become increasingly important to understand if concerns about the costs of cybersecurity stifle digital growth. Shocks induced by staggered passages of state-level security breach notification laws (SBNLs) provide a quasi-experimental setting to study this question. Since IT service firms are the main suppliers of digital goods and services, essay 3 studies how the enactment of SBNLs affects the employment of IT service providers (RQ3).

The three essays will add to the literature on several fronts. Essay 1 highlights the important role of cybersecurity labor in leveraging cybersecurity investments, and links recent studies on the substantive use of security technology (Angst et al. 2017; Kwon and Johnson 2018) with studies on

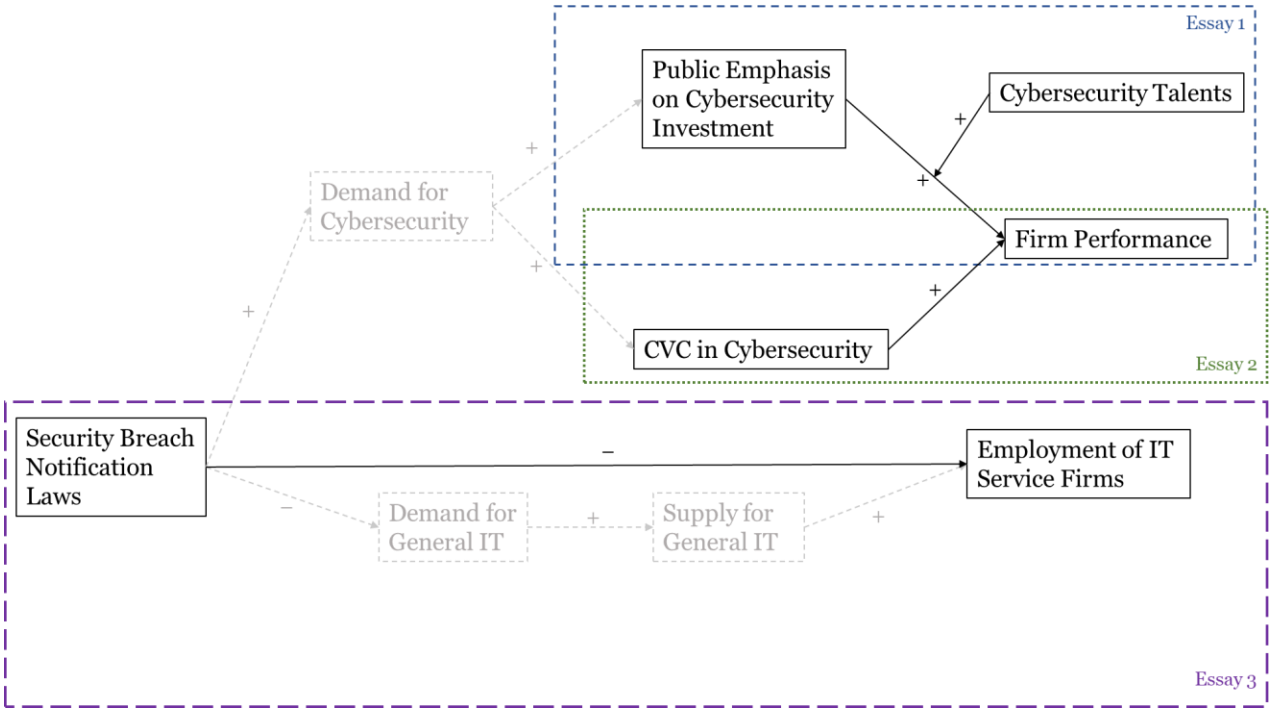
the business value of cybersecurity investments (Bose and Leung 2019; Gordon et al. 2010). Essay 2 unfolds the business value of innovation in cybersecurity as an area that is traditionally considered to be costly but not value-generating, thus extending cybersecurity literature beyond commoditized cyber products and services. Essay 3 provides fresh evidence related to the unintended and broader economic consequences of cybersecurity legislation and adds to the digital economics literature that has traditionally focused on cost reduction through digitization (Goldfarb and Tucker 2019). Table 1.1 summarizes the research questions, theory, methods, and findings. While the three essays cover a wide range of topics in cybersecurity, they are inherently linked through the supply and demand of cybersecurity and that of general IT. Figure 1.1 presents an overview of the dissertation.

Table 1.1. Overview

	Essay 1	**Essay 2**	**Essay 3**
Title	Cybersecurity talents and cybersecurity investments	Corporate venture capital in cybersecurity	Cybersecurity legislation and digitization
Research Question	How does cybersecurity labor impact the value of cybersecurity investment?	How does CVC investment in cybersecurity impact the value of the investing firm?	How does the enactment of SBNL impact employments by IT service firms?
Theory	Firm Legitimacy, BTOF	Real options	Supply and demand
Methodology	Instruments, Matching	Fixed Effects	Difference-in-differences
Data	*Cybersecurity investments*: Hand-collected from annual reports *Financial variables*: archival *Cybersecurity talent*: online social media	*CVC investments*: Crunchbase *Financial variables*: archival	*Employment*: Quarterly Workforce Indicator *SBNL*: Perkins Coie
Findings	a) Cybersecurity investments (CIs) create positive values as measured by Tobin's q. b) CIs accompanied by security talent recruitments generate significantly higher gains. c) CIs are more profitable for underperforming firms (breached firms in industries with less frequent breaches) and overperforming firms (un-breached firms in industries with more frequent breaches).	a) CVC investments in cybersecurity are associated with positive firm values as measured by Tobin's q. b) CVC investments in cybersecurity are associated with higher values for IT firms. c) More recent cybersecurity CVCs (2013-2017) are associated with higher values.	a) Employment by large and mature IT service providers decreases following enactments of state-level security breach notification laws. b) No significant impact on employment in smaller and younger IT service firms.

Notes. *CVC stands for corporate venture capital. BTOF stands for the behavioral theory of the firm. SBNL stands for security breach notification law.*

Figure 1.1 Relationships among the essays



CHAPTER II: CYBERSECURITY TALENT AND CYBERSECURITY INVESTMENTS[1]

2.1 Introduction

The rise of cybersecurity incidents has raised the broad-level visibility to cybersecurity issues and has significantly engaged top executives. Over time, cybersecurity has transformed from an operational level issue to a perennial strategic topic that engages key internal (e.g., executives) and external (e.g., stakeholders) agencies. Despite this strategic elevation of cybersecurity in corporations, the strategic value of investing in cybersecurity investments is yet to be fully understood. Absent such critical information about the strategic value of cybersecurity investments, the alerted executives may not have the right answers to champion for and incentivize those investments. Borrowing from the literature on strategic management (e.g., Wernerfelt 1995; Barney 2001) and the strategic value of IT (e.g., Wade and Hulland 2004; Wade and Nevo 2010), we contend that a clear understanding of the strategic value of cybersecurity investments requires answering three key questions. First, it should be clarified whether the various forms of cybersecurity investments create long-term business impacts that extend beyond the less stable, short-term market reactions (Q1). The second question pertains to whether those investments create firm-specific benefits (Q2). Finally, the third question is related to the strategic contingencies of value creation by those investment (Q3). Ongoing research on the value of cybersecurity provides knowledge that can be instrumental in initiating a discussion about the strategic value of cybersecurity investments. Nonetheless, the answer to these three questions cannot be extrapolated from the existing research.

[1] We thank the editors and anonymous reviewers at MIS Quarterly, and the participants at the 2018 AMCIS and 2018 BigXII+ MIS Research Symposium.

The existing research on the value of cybersecurity investments (VCI) has aptly documented its preventive value (e.g., Kankanhalli et al. 2003; Kwon and Johnson 2014; Angst et al. 2017; Kwon and Johnson 2018). Moreover, there is evidence pointing to the business value of specific types of cybersecurity investments – e.g., investment in identity theft countermeasures (Bose and Leung 2013; Bose and Leung 2019) – but not the broader set of cybersecurity investments. There is also evidence regarding the short-term returns to the broader set of cybersecurity investments (e.g., Chai et al. 2011). However, evidence regarding the long-term business impacts of the broader set of cybersecurity investments is lacking. Further, although some evidence exists (e.g., Bose and Leung 2019) about the forward-looking value of specific types of cybersecurity investments, it is not yet clear if those forward-looking assessments of value creation translate into durable impacts as shown in robust, book-keeping measures of value, such as return on assets (ROA) or return on sales (ROS). Therefore, empirical evidence that can directly answer Q1 is still lacking. Since the literature does not offer a direct answer to Q1, information about the specificity of the durable value of the cybersecurity investments (Q2) and the contingencies of the created value (Q3) is also lacking.

To answer these questions, we start by recognizing that although investments in cybersecurity do not appear to have an immediate pathway to profit, due to their risk-reducing nature and general treatment as an expense (Gordon and Loeb 2002), the legitimacy view (Bitektine and Haack 2015; Ginzel et al. 1993; Suchman 1995) can explain the strategic rewards gained from these investments. This view explains the impact of these investments through earned legitimacy, elevated levels of market trust, and subsequently, lower costs of accessing equity and debt, which hereafter we refer to as the cost of capital (Arthur 2003; DiMaggio and Powell 1983; Doh et al. 2010; Ho et al. 2017). The legitimacy view ties cybersecurity investments into a strategic source of impacting a firm's value, i.e., stakeholders, and a critical resource that impacts the competitive survival of the firm, i.e., capital. Because stakeholders are external observers of the firm and require the public transmission of

information about cybersecurity investments, we build on the previous literature (Gordon et al. 2010[2]) to argue that publicly emphasizing cybersecurity investments (PECIs) creates legitimacy rents for a firm by reducing its significant risks and lowering the cost of capital. Then, to further understand the heterogeneity in such rents, we build on the core tenet of the legitimacy view: "legitimacy is a generalized perception or assumption that the actions of an entity are *desirable, proper, or appropriate* within some *socially constructed system* of norms, values, beliefs, and definitions," (Suchman 1995, p. 574; emphasis added). This widely accepted definition of legitimacy (Bansal and Roth 2000; Bitektine and Haack 2015; Mitchell et al. 1997; Suddaby and Greenwood 2005) highlights the elements of *desirability* and *relative value* as the main characteristics of actions that boost legitimacy.

In the context of cybersecurity, the strategic *desirability* of PECIs is determined by their effectiveness in mitigating firm-specific cyber risk and security breaches. Cybersecurity talent is essential to turn general-purpose technological investments into solutions that fit the idiosyncratic cyber needs of the firm. As such, they facilitate substantive use of security technologies and algorithms and reduce subsequent data breaches. Conversely, there is an increasing shortage in the supply of cybersecurity talent[3] that makes firms successfully recruiting cybersecurity talent distinct in accessing a rare and critical complementary resource. So, PECIs accompanied with sufficient cybersecurity talent will be deemed more desirable by investors who lend capital (in the form of equity or debt) to a firm. Interpreting the desirability of PECIs by considering cybersecurity talent sheds light on the extent to which cybersecurity investments create firm-specific value (answering Q2), because: a) talent is the agency of innovation and firm-specific solutions (e.g., Schumpeter

[2] While Gordon et al. (2010) focus on voluntary disclosures about cybersecurity, our conceptualization is focused only on disclosures about cybersecurity investments and does not include other disclosures such as those pertaining to ongoing or recent breaches.

[3] For instance, an annual survey of IT professional by the Enterprise Strategy Group (see a summary here: https://www.csoonline.com/article/3331983/the-cybersecurity-skills-shortage-is-getting-worse.html) suggests that in 2018-2019, 53 percent of organizations report a problematic shortage of cybersecurity skills (up from 42 percent in 2015-2016). Moreover, a report by Gartner (2018; https://www.gartner.com/en/doc/3566417-adapt-your-traditional-staffing-practices-for-cybersecurity) suggests that the stagnant cybersecurity budgets and ever-increasing cybersecurity salaries mean that "the average security budget will not be enough to close the talent gap that exists."

1934), and b) the shortage in supply of cybersecurity talent, itself, adds to the specificity of PECIs when its value critically depends on successful recruitment.

The second element of increasing the legitimacy of cybersecurity investments, *relative value*, will be determined by institutional norms. Building on previous research on the behavioral theory of the firm (BTOF) (Cyert and March 1963) and theories on hacking motivations (Leeson and Coyne 2005; Ransbotham and Mitra 2009), we posit that security vulnerabilities of the firm relative to the industry average can potentially influence the heterogeneity in the business value gains of cybersecurity investments and the talent that supports it. Specifically, we extend the work by Ho et al. (2017), which posits that the market value of general IT investments is often interpreted relative to industry benchmarks. One key observation that necessitates the consideration of industry benchmarks when studying the VCI is that there are increasing reports suggesting in markets plagued with frequent security incidents, investors may become numb to subsequent news related to cybersecurity (Gordon et al. 2011; Kvochko and Pant 2015; Sen 2018). Therefore, investors' propensity to reward a firm's PECIs is likely to be influenced by news about other actors in the same market. Interpreting the relative value of PECIs by considering the security vulnerability of the firm relative to its industrial peers sheds light on the strategic contingencies of value creation by PECIs (answering Q3) as it ties the business value to the strategic context in which a firm competes.

In studying Q1-Q3 empirically, a matched sample of publicly emphasized cybersecurity investments is constructed based on public firms' reports filed with the Security and Exchange Commission (SEC) as well as their press releases. The success in recruiting cybersecurity talent is assessed based on an extensive proprietary labor dataset that contains information about 70 million resumes of workers in the US. The economic impacts of PECIs are tested in industries with different levels of security breaches in a sample of 3,130 firm-year matched observations, spanning from 2005 to 2015. The results reveal a generally positive (negative) impact of PECIs and cybersecurity talent recruitment toward the contemporaneous values of Tobin's q (cost of capital), as well as the lagged

values of ROA and return on sales ROS. More importantly, we unfold that success in attracting cybersecurity talent has a significant impact on the business value accrued from PECIs. These direct and indirect (interacting) impacts are stronger for over-performing (un-breached firms in industries where breaches are more frequent) and under-performing firms (breached firms in industries where breaches are less frequent). We also find that PECIs, together with talent recruitment, are effective in reducing subsequent cybersecurity hazards and that the cybersecurity vulnerability of the firm relative to its industry peers also impacts the marginal hazard-reduction benefits.

This study makes several contributions to the literature. First and foremost, this paper extends the recent studies highlighting the importance of substantive or actual use of security technology (Angst et al. 2017; Kwon and Johnson 2018) and the impact of IT talent (Tambe 2014; Wu et al. 2019), and reveals the importance of cybersecurity talent inputs in substantively supporting PECIs. This research builds on and extends the work by Angst et al. (2017), who suggest that the institutional substantiveness of investments determines the *preventive value* of organizational cybersecurity investments. While Angst et al. (2017) importantly posit that the *general characteristic* of a firm, such as its size, entrepreneurial orientation, and age, impact how a firm is capable of reaping value from its cybersecurity investments, we conceptualize the extent of recruitment of cybersecurity talent as a *cyber-specific characteristic* of the firm that determines the *professional substantiveness* of cybersecurity investments. Moreover, we extend the concept of industry benchmark in the general business value of IT (BVIT) literature (Ho et al. 2017) and contextualize it into the VCI literature – which has generally overlooked the impact of the industry. Specifically, we conceptualize and empirically model the security vulnerabilities of the firm relative to the industry peers as a vital strategic boundary condition that further explains the value accrued from cybersecurity investments. Finally, we extend the literature that has highlighted the business value of cybersecurity investments (e.g., Bose and Leung 2019), albeit by only considering forward-looking measures of business value (e.g., Tobin's q, market reactions), and show that: a) the market benefits observed in forward-looking indices later extend to the more book-keeping measure of value such as return on assets (ROA) and

return on sales (ROS), and b) the reduction in cost of capital may explain the link between the observed risk reduction benefits of cybersecurity investments and the subsequent business value benefits.

2.2 Theory development

2.2.1 The preventive value of cybersecurity investments

Empirical studies on cybersecurity investments have documented the preventive value of these investments by studying their impact on reducing a firm's cybersecurity risks. A pioneering survey study showed that deterrent security administrative procedures and preventive security software reduce computer abuse (Straub 1990). Another survey study emphasizing managerial support, industry type, and organization size also found deterrent efforts and preventive measures lead to enhanced information systems (IS) security effectiveness (Kankanhalli et al. 2003). More recently, an archival study using firm announcements revealed that attaching risk-mitigation themes to security risk disclosures in annual reports are followed by fewer subsequent breach announcements (Wang et al. 2013).

In contrast to studies focusing on the voluntary practices in pursuing cybersecurity investments, the preventive value of these investments is also evaluated in mandatory settings, such as in the healthcare industry, wherein governmental agencies regulate and encourage relevant initiatives. Particularly, Kwon and Johnson (2013, 2014) showed that cybersecurity investments in mandatory settings could have mixed preventive results. They found that in operationally immature hospitals, compliance with security regulations significantly reduces data breaches, whereas the effect vanishes for operationally mature hospitals (Kwon and Johnson 2013). They also found that proactive security investments (not motivated by regulations) in hospitals are associated with lower security failure rates, where external regulatory pressure weakens the effect (Kwon and Johnson 2014).

Finally, moving beyond a nominal view of cybersecurity investments, two recent studies addressed the role of investment substantiveness in mitigating threats. Specifically, Angst et al.

(2017) showed that only substantive cybersecurity investments in hospitals could effectively reduce data breaches. Relatedly, Kwon and Johnson (2018) found that meaningful-use attestation of security technology is effective in mitigating certain types of cyber threats in hospitals.

2.2.2 The business value of cybersecurity investments: a legitimacy view

The role of cybersecurity investments in risk reduction is far more explained than its role in creating business value. This lack of clarity about their business value is in part due to the nature of cybersecurity investments. While investing in factors directly involved in production and selling of goods and services (e.g., capital, R&D) has a clear path to productivity, organizations are sometimes faced with decisions about certain categories of investment, such as investments in cybersecurity, that are not direct inputs or throughputs of sales or production. Yet, these investments are important because of their risk-reducing impact on matters important to stakeholders (Karnani 2011). Literature in strategic management suggests that organizational investments with a risk-reducing nature, such as those related to corporate social responsibilities, can generate positive financial performances through the enhancement of firm legitimacy (Cochran and Wood 1984; McWilliams and Siegel 2001). Such legitimacy creates value through an important pathway: reduction in the firm's cost of capital.

That legitimacy is evaluated by stakeholders is pertinent in explaining this pathway to creating business value for the firm. Specifically, stakeholders are key actors in providing capital resources to a firm, in the form of equity or debt (Sharfman and Fernando 2008), and therefore, regulate a firm's cost of capital. In regulating these costs, stakeholders consider both current and future risks that they deem important in the economic and business well-being of the firm (Sharfman and Fernando 2008) and lower the rates charged for accessing capital for firms that have reasonably lower risks. For instance, although investments with a significant externality, such as environmental risk management investments, appear to have an immediate cost nature to most firms, not committing to them increases the risks of litigation by governmental and non-governmental entities and the risks of reputation loss (King and Shaver 2001), and subsequently, increases the cost of capital (Sharfman and Fernando

2008). Since capital has long been and continues to be an important resource in the production and sales processes of a firm (Coma and Douglas 1928; Lemmon and Zender 2019), reducing the costs in accessing it renders the firm a critical resource at a lower premium and enhances its gains.

The legitimacy of organizational initiatives is often gauged by evaluating the extent to which firm activities agree with the relevant expectations. In the context of cybersecurity, the widespread expectation is that firms should maintain information confidentiality, integrity, and accessibility (Von Solms and Van Niekerk 2013). Consequently, investing in cybersecurity tends to agree with this expectation, and hence publicly emphasizing it, will increase firm legitimacy. Specifically, PECIs of a firm will draw stakeholders' attention because these activities will determine the firm's information security level, which will, in turn, affect the immediate interests of those stakeholders.

Security breaches reduce trust (Acquisti et al. 2006; Cavusoglu et al. 2004) and erode reputation, incur costs of litigation and fines, and may force a firm to engage in strategic shifts to remediate the damage. Stakeholders following a firm's business performance take into consideration these aspects when evaluating the riskiness of the firm's prospect and determining the cost of capital for the firm. The evaluation of the cybersecurity damage following security breaches is best exemplified in Standard and Poor's report downgrading the 'BBB+' rating outlook of Equifax Inc. to negative, following the announcement of its cybersecurity incident in May-July 2017:

> *"…we believe the company faces meaningful costs related to lawsuits and potential government investigations… Further, we project that Equifax will see some pressure on its operations over the next 12 to 18 months. In particular, the company's Global Consumer Solutions business (13% of 2016 revenue) could see steep revenue declines since it derives a large portion of revenues from the U.S. consumer credit protection service. Finally, the incident also poses reputational risk that would have an impact on its other lines of business albeit to a lesser extent…"*

To counter the current or future adverse impacts, cybersecurity investments can restore or increase trust in the firm and enhance its legitimacy. However, due to the externality of the agency evaluating these investments (i.e., stakeholders), broadcasting these initiatives is critical. A public

firm formally broadcasts its cybersecurity investments via the official reports filed with the SEC. While some may question the sincerity of such reports, it is worth noting that these documents have legal consequences, where shareholders have the right to sue a public company if there is a significant discrepancy between their promises and actions (Rogers et al. 2011). Hence, stakeholders have good reasons to react correspondingly to PECIs, thereby increasing the legitimacy and valuation of the firm (Zajac and Westphal 2004), which in turn will be met with economic rewards. Therefore, under the tenets of the legitimacy view, and consistent with prior literature (Bose and Leung 2019; Chai et al. 2011; Gordon et al. 2010)[4], we posit the following as our baseline hypothesis:

> **Hypothesis 1:** Public emphasis on cybersecurity investments creates positive business values for the investing firm.

2.2.3 Substantiveness and the desirability of cybersecurity investments

The tenets of organizational legitimacy theory (Suchman 1995) assert that organizational actions create legitimacy only if they are deemed desirable. The existing literature on the preventive value of cybersecurity investments (e.g., Angst et al. 2017) has already unfolded the critical importance of substantive cyber investments in reducing data breaches. As such, stakeholders would assess substantively supported PECIs more desirably than ones that are not, since those unsupported actions do not reduce the risks that matter to stakeholders.

As with any organizational investment, the success of cybersecurity investments relies on various organizational support, among which the provision of technical labor is perhaps the most fundamental. Specifically, acquiring human talent with expertise in cybersecurity allows leveraging generic technological assets and solutions, e.g., intrusion detection systems and anomaly detection algorithms, and turning them into idiosyncratic solutions. The knowledge-based view of the firm

[4] We acknowledge that this hypothesis has similarities with the existing literature (i.e., Bose and Leung 2013, 2019; Chai et al. 2011); however, our empirical examination of this hypothesis differs in two distinct ways: a) our examination considers a broader range of investments, not only limited to a specific technological investment such as intrusion detection (departing from Bose and Leung 2013, 2019), and b) our assessment of business value extends beyond forward-looking or short-term indices of value and also includes important book-keeping indices such as cost of capital, ROA, and ROS (departing from Bose and Leung 2013, 2019; Chai et al. 2011).

positions human talent in a key role (Felin and Hesterly 2007) to integrate the knowledge about the organization, its legacy systems, and unique cybersecurity threats with the knowledge about general-purpose assets, such as cybersecurity solutions. Since technical know-how is embedded in IT labor, which will shape the return on IT investments (Tambe 2014; Tambe and Hitt 2013), security talent will heavily influence the outcomes of cybersecurity investments. The essential role of IT labor in IT productivity has been documented in BVIT literature. On top of its direct contribution to productivity (Brynjolfsson and Hitt 1996; Tambe and Hitt 2012), IT workforce complements other IT investments (Melville et al. 2004; Tambe 2014; Wu et al. 2019).

As the landscape of a firm's information and enterprise systems evolves in response to its idiosyncratic needs, existing cybersecurity measures will require reviewing, updating, and swift adaptations. Moreover, cybersecurity threats to a firm are not only shaped by idiosyncrasies that arise from the uniqueness of internal legacy systems and specificity of a firm's vulnerabilities. Rather, the cyber risks of a firm are also intertwined with its broader institutional context. Negative externalities, dynamics of its peer institutions' cybersecurity strategies, and their extended history of previous attacks and imminent threats (Haislip et al. 2019; Jeong and Lee 2019; Sen and Borle 2015) all can interactively impact the cybersecurity risks and required responses in the firm, adding to its cybersecurity specificity and idiosyncrasy. Therefore, such a degree of idiosyncratic risks, as perceived by stakeholders, emboldens the importance of human talent in inventing ways to utilize a set of general-purpose solutions and apply them to firm-specific threats.

Without a commitment to investment in cybersecurity talent, a firm can barely paint itself as an institution well-equipped to counter or remediate cyber threats. Considering the increasing utilization of online job search platforms for recruitment purposes and the popularity of professional social media platforms such as LinkedIn, investors are increasingly aware of a firm's talent recruitment efforts. Hence, when a firm hires cybersecurity personnel, it signals its intention to substantively implement and assimilate its PECIs rather than merely symbolically broadcasting them. Possessing skilled personnel is essential in effectively using those investments, and hiring involves significant

contractual and other long-term commitments by the firm. Thus, stakeholders view cybersecurity talent as a substantive complement to PECIs to reduce cyber risks. This will increase the firm's legitimacy and ultimately boost firm value:

> **Hypothesis 2:** Cybersecurity talent recruitment enhances the positive association between publicly emphasizing cybersecurity investments and business value.

2.2.4 The relative value of cybersecurity investments

The legitimacy of a firm's actions are often interpreted contingently in a socially-relative fashion (DiMaggio and Powell 1983; Kostova and Zaheer 1999). That is, the legitimacy of organizational actions are evaluated by considering how those actions impact the firm relative to its industry peers (Doh et al. 2010). The behavioral theory of the firm (BTOF) (Cyert and March 1963) suggests that rational decision-makers, learning from repeated economic and market transactions and feedback loops, often engage in actions that either help a firm under-performing its aspirations reach its desired objectives (i.e., problemistic search) (Argote and Greve 2007; Miller and Chen 1994), or allow a firm over-performing its aspirations to keep its superior position (i.e., slack search) (Greve 2003b; Nohria and Gulati 1996). Notably, under- and over-performing relative to goals defined in the institutional context (i.e., social aspirational gaps) are identified as drivers of key organizational actions. Numerous studies have reported empirical support for both problemistic and slack searches as the basis for rational organizational actions such as increasing R&D budgets (Greve 2003a), finding new strategic partners (Baum et al. 2005), and acquiring another firm (Iyer and Miller 2008). Since these rational actions are learned from and reinforced by the feedback received from the markets and stakeholders (Cyert and March 1963; Levitt and March 1988), it is plausible to assume that actions pertaining to either problemistic or slack search are deemed more legitimate relative to those that do not fall into either category.

Therefore, the pursuit of PECIs by firms under- or over-performing relative to the cybersecurity of peer firms may be deemed more legitimate by stakeholders. Additionally, exercising PECIs when a

firm is on par with its rivals may be viewed as less necessary, and therefore, met with fewer legitimacy rents. In an industry where security breaches are highly frequent, an un-breached firm is considered over-performing relative to its institutional environment, whereas a breached firm is considered performing as expected (on-par firm). In an industry where security breaches are less frequent, a breached firm is under-performing, whereas an un-breached firm is performing as expected (also, on-par firm).

The broad social relativity expectations extrapolated from BTOF also align with reasons specific to the cybersecurity context. That is, over- and under-performing firms potentially face greater cybersecurity risks relative to the firms performing on par with their industry. Therefore, the marginal value of PECIs and substantive talent recruitments supporting them are higher, due to the bigger risk they mitigate. The reasons for higher risks faced by under- and over-performing firms relative to on-par firms, as perceived by stakeholders, are rooted in the motivations and enablers that instigate security breaches.

Existing research on motivations of outsiders with malicious intent orchestrating security breaches (hereafter, hackers) shows that they are either driven by profit or fame (Leeson and Coyne 2005). Profit-driven hackers determine their targets based on cost-benefit analyses (Cremonini and Nizovtsev 2009); fame-driven hackers determine the targets based on the degree of fame and joy of successful hacks. Hackers have been shifting their focus toward financial gains, and profit-driven hackers tend to inflict more damages than fame-driven ones (Sieberg 2005). Moreover, the existing research suggests that knowledge about organizational cyber vulnerabilities are often disseminated in dark forums and networks such as Darknet and Deepnet sites (e.g., Jordan and Taylor 1998; Benjamin et al. 2016). These vulnerabilities often go on dark market sales5. Like any other product, the value of these exploitations is determined by the characteristics of the target and the value that the exploitation

[5] For example, FireEye, a major cybersecurity firm, identified an exploit for a Windows vulnerability (MS15-010/CVE 2015-0057) being sold on a darknet market for 48 BTC (around$10,000-15,000; April 2015), eventually tracing this vulnerability being exploited by Dyre Banking Trojan to steal credit card information in July 2015.

can yield. For an under-performing firm (i.e., breached in industries with a low frequency of breaches), two factors make their cybersecurity exploitation a low-cost mission to hackers, and therefore, increase their attractiveness to hackers. First, the relative unimpactedness of other firms in the industry signals that focusing on the already breached firm may require less effort to find fresh exploitations. Second, the already disseminated information about the exploited vulnerability can be leveraged again at a lower premium than its initial sales value. Therefore, an under-performing firm becomes a low-cost target and will be at a heightened risk relative to its peers, in the same industry, that are unexploited. This increased risk of re-exploitation is recognized by stakeholders and raises their sensitivity to PECIs by under-performers, leading to higher marginal value from PECIs gained by under-performers.

Albeit for different reasons, over-performing firms (unbreached in industries with a high frequency of breaches) are also more attractive targets relative to their peers. In an industry with frequent breaches, an over-performing firm is a target with a higher yield than a firm performing as expected (breached) because the breached information from on-par firms (i.e., its customers' credit/personal information) is likely already available in the black market, hence less valuable. More importantly, frequent breaches in the environment suggest low attacking cost or high attacking yield, or both. In either case, profit-minded hackers will be more willing to tap into unbreached firms when there are more breaches in the environment: the knowledge externalities of similar attacks to breached peers reduce the costs of attacking the unbreached firm, and the unbreached status of the firm increases the yield of a potential exploit (since, for instance, exploited information about customers of an unbreached firm is not readily traded in black markets, and hence, is of more value to buyers). For fame-driven hackers, over-performing firms may be particularly enticing targets since the utility (e.g., fame, sense of achievement) gained from breaking into an un-breached firm is much higher than exploiting previously breached firms. Attracting both profit- and fame-driven hackers, over-performers are expected to move first and signal their superior protection through cybersecurity investments to deter attacks (Cavusoglu et al. 2008; Cremonini and Nizovtsev 2009). Stakeholders

recognizing the higher future risks to over-performers, relative to their already-breached peers, will then reward PECIs by over-performers at a higher rate. Put together, we posit the following:

> **Hypothesis 3:** The increase in business value as a result of emphasizing cybersecurity investments is greater for under-performing and over-performing firms relative to their peers.

In discussing the complementary role of human talent in increasing value creation with PECIs, we explained that supporting talent is deemed essential by stakeholders to leverage general investments and turn them into idiosyncratic solutions. Therefore, the perceived value and necessity of human talent in leveraging PECIs increases as does the firm's need for idiosyncratic cybersecurity solutions. Both under- and over-performing firms show more unique risk patterns relative to their peers in the same industries. Therefore, under- and over-performing firms are perceived more idiosyncratic in their cybersecurity needs, as they get evaluated by stakeholders.

An under-performing firm requires solutions that uncover why, in a low-risk environment, the firm has emerged as a target to ensure such anomalies do not happen again. Moreover, relative to their unbreached peers, under-performing firms have to engage in additional screening that ensures the dissemination of their unfolded vulnerabilities is contained, to avoid secondary exploitations. Therefore, stakeholders do not view common solutions followed by safe peers as sufficient responses by under-performers.

For over-performing firms, their strong position relative to other peers alludes to the presence of idiosyncrasies that make hackers' disseminated knowledge about vulnerabilities of other firms less applicable to them. But such a privileged position may not be sustainable as hackers continuously build on their gained knowledge from the vulnerabilities of the breached peers of over-performers. Therefore, stakeholders expect over-performing firms to continue to bring in human talent that can keep up with changes to the information systems portfolio of the firm and maintain its security idiosyncrasies relative to its institutional peers. Further, as over-performers stand out as cyber-security leaders among struggling peers, they must deal with a higher frequency of fame-driven

exploitation efforts. Therefore, they have to develop cybersecurity capabilities that are different from those possessed by peers under less strain for fame-driven attacks. Also, their exposure to both types of profit- and fame-driven exploitations makes their portfolio of risks dissimilar to their peers. Put together, the idiosyncratic cybersecurity needs of under- and over-performing firms relative to their peers make the support of human talent an even more critical complementary input in the eyes of stakeholders. Stakeholders recognizing these idiosyncrasies would, therefore, reward the complementarities between PECIs and recruiting cybersecurity talent at a higher rate. Thus:

> **Hypothesis 4:** The increase in business value as a result of the interaction between emphasizing cybersecurity investments and recruiting cybersecurity talent is greater for under-performing and over-performing firms relative to their peers.

2.3 Method

2.3.1 Data and sample

In creating our initial sample (Sample I), we followed the guidelines by Gorodon et al. (2010) and obtained SEC disclosures of public firms, from 2005 to 2015. A firm was kept in the sample only if: all of the firm's financial information was available, if its book value was positive, and if the firm's industry classification was not missing. This resulted in 99,904 firm-year observations belonging to 6,244 pubic firms. Then, a dataset on publicly announced security breaches and emphasized cybersecurity investments is constructed by conducting a keyword search among news sources from 2005 to 2015 on Lexis-Nexis. Sample search terms include cybersecurity, security, phishing, etc. (See Appendix A for a complete list of keywords). Two research assistants compiled the news releases to: a) eliminate duplicate announcements, b) eliminate irrelevant announcements, and c) categorize the announcements into two broad groups of breaches or cybersecurity investments. The three tasks' convergence rates for the two research assistants are 98%, 91%, and 87%, respectively. In a subsequent round, the disagreements were resolved by revisiting the initial schemes and definitions

relevant to the study. This process yielded 2,884 announcements about cybersecurity investments made by 1,673 firms (Sample A_0) and 4,871 announcements about security breaches by 3,978 firms (Sample B_0). Data breach incidents are also supplemented by records from the Privacy Rights Clearinghouse website (www.privacyrights.org).

Therefore, only a limited number of firms in our sample (i.e., 26 percent) experienced at least one publicly announced cybersecurity investment in the span of 16 years covered in the study. It is then conceivable to assume that some unobserved factors influence the selection of a firm into our target treatment (i.e., publicly announced cybersecurity investments). As such, the comparison between the self-selected treatment firms and those that did not self-select may lead to biased estimates because of the conflation of the treatment with the unobserved self-selection factors[6]. Hence, although we start our empirical presentation of our findings by focusing on Sample I, we further pruned Sample I to construct a matched sample that attenuates such biased comparisons.

Since examining H3 and H4 requires creating subsamples based on the relative vulnerability of the firm, we start building our matched sample by estimating the extent of the occurrence of security breaches in the industry in which each observation in Sample A_0 (i.e., firms with at least one year of treatment) is active. Therefore, the initial set of announcements about security breaches (Sample B_0) is reduced to publicly-traded firms and then matched to at least one represented industry in Sample A_0, based on two-digit SIC codes. The reduced sample contains 2,717 firm-year security breach announcements made by 2,308 firms (Sample B). Based on data from Sample B, we divide the Sample A_0 industries (based on two-digit SIC codes) into ones with a high and low frequency of breach (based on a median split of the frequency of breaches happening in each industry in a given year, utilizing information from Sample B), and categorize each firm-year observation in A_0 into one of the following subsample categories: **SS1)** breached in a low-frequency industry (under-performing), **SS2)** breached in a high-frequency industry (performing on par in high risk), **SS3)** not

[6] Put differently, an unrestricted sample's estimates are potentially biased as the extent of PECIs does not reasonably exogeneously vary, and the choice of PECIs is restricted for some firms, but not for the others.

breached in a low-frequency industry (performing on par in low risk), and **SS4)** not breached in a high-frequency industry (over-performing). The main estimations of the study are run separately in each subsample. Table 2.1 summarizes the description of each subsample.

Table 2.1 Subsample Classifications

	Low breach frequency in industry	High breach frequency in industry
Breached	(SS1) Under-performing firms	(SS2) On-par firms (high-risk industry)
Un-breached	(SS3) On-par firms (low-risk industry)	(SS4) Over-performing firms

To balance the sample of treated firm-year observations (Sample A_0) with proper counterfactuals, we look for untreated observations from the same firm in an adjacent year (t+1 or t-1) that satisfy two conditions: a) the firm does not publicly announce a cybersecurity investment in that adjacent year, and b) the firm's categorization into the four mentioned subsamples remains unchanged across the treated and control (adjacent) years. This matching procedure ensures that our comparison between the treated and untreated observations is less biased since the sample of counterfactuals is also selected from the firms that, in close chronological proximity (i.e., a year), can undergo, or have undergone, the treatment. This matching procedure also allows us to remove the firm-specific time-invariant heterogeneities. After this matching process, 3,130 firm-year observations (1565 pairs of treatment and counterfactuals) belonging to 582 unique firms (Sample A) are retained for the analysis. For each firm-year observation in Sample A, cybersecurity talent recruitment data are obtained from a proprietary dataset of over 70 million online resumes that are posted from 2008 to 2017 and supplemented by a major online employment-related search engine.

2.3.2 Measures

Following previous business value of IT literature (Bharadwaj et al. 1999; Chari et al. 2008), the business value of cybersecurity investment is primarily measured by considering Tobin's q ratio[7]. As a forward-looking measure of firm value, Tobin's q is less sensitive to accounting practices and is appropriate for the evaluation of IT-related investments (Chari et al. 2008). In the security context, Angst et al. (2017) pointed out that the benefits of substantive adoption will take time to be realized,

[7] Later, we examine the impacts of the forward lags of ROA and ROS.

making Tobin's q the proper contemporaneous measure of value. When Tobin's q is higher than 1, the long-run equilibrium market value is greater than the book value of the firm, signifying an unmeasured source of profit (Bharadwaj et al. 1999). Following Chung and Pruitt (1994), **Tobin's q** is calculated as q = (Market value of common stock + liquidating value of preferred stock + liabilities)/Total assets.

A firm's **PECIs** in year t is measured by considering the emphasis on the investments in SEC filings[8]. Various Securities and Exchange Commission (SEC) reports (10-K, 10-Q, 8-K, 8-K/A) for the 3,130 observations from sample A were collected from SEC's EDGAR database[9]. Paragraphs containing the keywords pertaining to cybersecurity investments were highlighted automatically, by a search engine, and manually confirmed by two research assistants. Adapting the measure of IT emphasis in SEC reports from Steelman et al.'s (2019) work, PECIs is calculated as the natural log of the ratio of paragraphs about cybersecurity investments to the total number of paragraphs in that year's SEC filings[10]. Although SEC documents filed by a firm are a critical source to relay key information about cybersecurity investments of a firm, other press releases likely provide more depth and information to stakeholders. As such, in a subsequent analysis, we also estimate our model with a measure of public release emphasis, which is a ratio of the number of cybersecurity-related public press releases by a firm in year t to the number of all of its public press releases in the same year.

The information about the cybersecurity talent recruitment **(TR)** is extracted from the employees' posted resumes (i.e., from the database of 70 million resumes). Particularly, to estimate the number of cybersecurity talent recruited by firm *i* in year *t*, we first searched the job positions sections of the resumes in our sample and count instances where an individual with cybersecurity expertise had

[8] This approach is similar to Gordon et al.'s (2010) approach, although unlike their 0/1 measurement, we use a continuous measure of emphasizing cybersecurity investments.
[9] The results of the study remain qualitatively unchanged when only 10-K reports are considered, as well as when the number of distinct investments is controlled for. These findings are discussed under the "Robustness tests" section.
[10] While most announcements and emphasis on them in annual reports mention investment in cybersecurity technologies (e.g., investment in encryption technologies) and investment in cybersecurity innovation (e.g., budget assignment to develop an in-house security labs, and investment in cybersecurity startups), we dropped 32 announcements and 78 annual report mentions that were directly linked to talent-related activities to avoid double-counting. Under the "Robustness tests" section, we present results of an estimation that explicitly includes the number of distinct technological (TECH) and innovational (INN) investments as covariates.

indicated starting a position in year *t* at firm *i*[11]. For instance, to identify cybersecurity talent recruited by Target Inc. in 2013, we searched our database for posted resumes of individuals where they had indicated starting a position at Target Inc. in 2013 and also had cybersecurity-related keywords mentioned in their roles and projects performed. This approach is similar to labor measures introduced and developed by Tambe and Hitt (2012).

Specifically, to identify a cybersecurity employee recruited by a firm in year *t*, we started with identifying sections of resumes that report an individual's previous positions or projects. Because different individuals design their resumes differently, a selected set of HTML versions of the online resumes (1000 resumes) were first manually mined to identify the header keywords that different individuals use to list their previous and current job positions. From this initial mining, a bag of header keywords was formed to identify the parts of a resume that detail job positions. Then, these identified sections of all the available resumes were searched to find matches with the set of firms in our sample to: a) determine if firm i in year t recruited a particular individual, and b) identify the cybersecurity expertise of that individual (and his/her extent of expertise based on the number of years of experience in a cybersecurity project/position).

To evaluate the cybersecurity expertise in each retained resume, we start by using a list of skillset keywords as indicated in Table A1 in the Appendix A. To categorize a recruited employee into the security-related IT labor group at year t, the employee's resume should report at least one job position or executed project, in periods before year t, where the title or the summary of the position/project (if any) contains the keywords related to cybersecurity. Since it is possible that our initial list missed other relevant keywords, such as more complicated bi- or tri-grams pertaining to security-related skills, we manually coded another set of 1000 resumes and categorized the individuals to those with cybersecurity skills and those without it. Then, this scored set was used as

[11] Since the names of employees posting their resumes are redacted in our database (to preserve idnividuals' identity and privacy, per the online platform's request), we took an additional step to ensure we do not double count employees that may have posted their resumes at two or more points of time. We ran a search to find exact matches of resumes based on previous employers and the educational history and removed those exact matches.

an input to a machine learning algorithm, by following Bai et al. (2004; see section 4.3 of this work for a sketch of the algorithm), to further identify the more complex, relevant keywords (including the more complex bi- and tri-grams). Once the machine-learning algorithm scored the retained resumes, another random sample of 1000 resumes was selected and manually coded. While we did not find any resumes that were misclassified as a skilled cybersecurity individual by the algorithm, we find 26 instances where an individual with cybersecurity talent was misclassified as non-cyber talent (misclassification rate: 2.6%). Given the lack of false positives and a misclassification rate below 5%, we proceeded with the classifications obtained from our machine-learning algorithm at this stage.

The extent of cybersecurity talent recruitment (**TR**) is measured by the natural log of the sum of recruited security-related IT employees, weighted by the number of years that each individual has been in projects/positions related to cybersecurity before recruitment, in a firm for a given year[12]. Following Tambe and Hitt (2012), we consider the talent movements unfolded by mining the resumes present in our database as a sample of the actual talent recruited by each firm. Since different firms can have a different rate of resume representation in our sample, we scale the raw values of TR by a firm-specific sampling rate, ρ, which is estimated as the number of all workers in all occupations in our data from a particular firm in a particular year divided by the number of all workers in all occupation for the same firm-year observation as reported in COMPUSTAT[13].

Since our dataset includes resumes of employees that actively look to change jobs, it is possible that our measure of TR is biased, as those employees may oversell their cybersecurity skills due to the demand for it. We have three reasons to believe that such a measurement error does not systematically bias the TR measurement. First, we aggregated our measure of TR by industry and

[12] Models that consider the pool of talent (existing + recruited) also show results that are qualitatively converging with the results based on this main measure. However, the models specified with TR show better fit indices, perhaps due further observability of the recruited talent, compared to the talent pool, in online job posting platforms where a firm's hiring activities become visible to investors.

[13] The results remain qualitatively similar when the weight of cybersecurity talent is based on the inverse of the Mahalanobis distance between the vector of cybersecurity keywords listed on the individual's resume and the cybersecurity keywords mentioned in the SEC filing of the firm in the year of recruitment. Due to the similarity of these estimates to our main estimates, we have not included them in the manuscript, but these results are available upon request.

compared the share of each industry in recruiting TR with the share of each industry in hiring "information security analyst" as reported by Bureau of Labor Statistics (BLS) and found a Spearman's rank correlation of 0.961. This high correlation suggests that the distribution of cybersecurity talent across industries in our sample is very close to the distribution of cybersecurity recruitment in BLS surveys. Although this is not direct evidence of cross-firm unbiasedness, it suggests a lack of bias in reporting TR across industries in our sample.

Further, we randomly selected profiles of 1000 IT employees on LinkedIn, working in at least one of the firm-year observations of our sample, and compared the extent of TR for those firm-year observations estimated based on the LinkedIn information with the extent of TR based on 1000 randomly-selected resumes form our proprietary dataset in the same fashion and observed a correlation of 0.767 between the two measures. Since LinkedIn is a professional networking platform, rather than an exclusive online job search engine, the high correlation between the measure of TR in our dataset and the one constructed from LinkedIn may indicate that individuals who actively seek to change jobs (and hence using an online job search engine) do not excessively oversell their skills. Our concerns are further attenuated because our measure of TR relies on traceable positions and projects that an individual reports, rather than merely relying on the skillset keywords listed in the resumes.

Finally, for each firm-year observation, we estimated the number of IT employees in our sample of resumes and compared this figure with the number of IT employees reported by the same firm-year in the Computer Intelligence (CI) database. We observed a Spearman's rank correlation of 0.914 between the two measures. Since IT skills, in general, are also considered to have an above-average demand, the high correlation between our measure of IT employment and the one obtained from the CI database suggests the overselling bias may not be distributed systematically across firm-year observations in our sample.

Apart from the **year** fixed effects, we also control for few other firm variables. Related **diversification** is evaluated by the entropy measure (Robins and Wiersema 1995) used in prior literature (Bharadwaj et al. 1999). We measure firm **size** as the natural log of the number of

employees in thousands. Total **assets** is measured using reported data from COMPUSTAT. **R&D** and advertising (**ADV**) expenditures are estimated using the ratio of the investment amounts divided by the firm's annual revenue, accessed from COMPUSTAT. Table 2.2 presents the correlation matrix, and Table 2.3 presents a summary of variables and their measurement.

Table 2.2 Correlation table

	Variable	Mean	Std. Dev.	1	3	4	5	6	7	8
1	Tobin's *q*	1.11	1.31							
2	PECIs	-5.60	-4.12	0.09						
3	TR	5.06	5.64	0.14	0.13					
4	Related diversification	0.17	0.32	0.03	0.03	-0.07				
5	Firm size	3.03	1.12	0.04	0.12	0.14	0.02			
6	Assets	0.48	0.18	0.22	0.11	0.18	0.01	0.22		
7	R&D	0.13	0.16	0.18	0.10	0.12	0.03	0.21	0.04	
8	ADV	0.02	0.02	0.05	0.11	0.15	0.06	0.14	0.05	0.04

Table 2.3 Variables and measurement

	Variable	Measure	Data Source
Dependent variables	Tobin's *q*	(Market value of equity + book value of inventories + liquidating value of preferred stock + long-term debt + net short-term debt) / total assets	COPMUSTAT, CRSP
	Return on Assets (ROA)	Net income / total assets	COPMUSTAT
	Return on Sales (ROS)	Operating income / net sales	COPMUSTAT
	Security Hazard	Estimated based on a cox proportional hazard model that uses the time of a security breach incident for a given firm as the failure time variable	Privacy Rights Clearinghouse, EDGAR
	Cost of Capital	Weighted average cost of capital (see Appendix C)	COPMUSTAT, Bloomberg financial
	Cost of goods sold	All expenses directly allocated by the company to production, such as material, labor, and overhead.	COPMUSTAT
Independent variables	Publicly Emphasizing Cybersecurity Investments (PECIs)	ln(number of paragraphs about cybersecurity investments / total number of paragraphs in SEC filings) (adapted from Steelman et al.'s (2019) measure of organizational commitment to IT)	EDGAR
	Talent Recruitment (TR)	ln(total number of employees recruited with cybersecurity talent, weighted by each employee's number of years of experience in cybersecurity roles/projects before recruitment) (the raw natural log measure is scaled by the firm-specific sampling rate, ρ, following Tambe and Hitt (2012))	Proprietary online resume dataset
	Press Release Emphasis (PRE), for robustness	Number of cybersecurity-related public press release/total number of public press releases	LexisNexis
Control variables	Firm Size	ln(number of employees in thousands)	COPMUSTAT
	Assets	Total assets	COPMUSTAT
	Diversification	Entropy measure as outlined in Robins and Wiersema (1995)	COPMUSTAT
	R&D	R&D expenditure / annual revenue	COPMUSTAT
	Advertising (ADV)	Advertising expenditure / annual revenue	COPMUSTAT

2.3.3 Estimation

For each of the subsamples in Table 1, we start with estimating the following equation:

$$q_{it} = \beta_1 \cdot PECIs_{it} + \beta_2 \cdot TR_{it} + \beta_3 \cdot diversification_{it} + \beta_4 \cdot size_{it} + \beta_5 \cdot asset_{it} + \beta_6 \cdot R\&D_{it} + \beta_7 \cdot ADV_{it} + YEAR + \epsilon_{it} + c_i \quad (1)$$

where subscripts i and t denote firm i in year t. ϵ_{it} is the error term, and c_i is the firm-specific time-invariant unobserved heterogeneity term. Further, in line with our theoretical discussion, we assume that $\beta_1$is influenced by TR. Therefore, we re-write (1) as the following:

$$q_{it} = \beta_1 \cdot PECIs_{it} + \beta_2 \cdot TR_{it} + \gamma_1 \cdot TR_{it} \times PECIs_{it} + \beta_3 \cdot diversification_{it} + \beta_4 \cdot size_{it} + \beta_5 \cdot asset_{it} + \beta_6 \cdot R\&D_{it} + \beta_7 \cdot ADV_{it} + YEAR + \epsilon_{it} + c_i \quad (2)$$

To estimate Equations (1) and (2), we treat PECIs, TR, and their interaction endogenous, since some unobserved time-variant factors may influence the set of these variables as well as the error term. Therefore, these variables are instrumented when estimating both equations using a panel two-stage least squares (2SLS) procedure.

To identify the set of appropriate instruments (X_{it}), we start with factors identified by Xue et al. (2012), which instrument generic investments in IT. Mainly, they use the firm's previous year IT investment (ex_IT), the industry IT investment (ind_IT) (from the Current-Cost Investment in Private residential Fixed Assets Table from the Bureau of Economic Analysis (BEA)), the industry tax ratio (Tax) (GDP-by-industry tables reported by BEA), the industry-operating surplus (Surplus) (from BEA's GDP-by-industry tables), the industry material-energy input ratio (MER) (calculated using BEA's value-added-by-industry tables), the industry service-energy input ratio (SER) (calculated using BEA's added-by-industry tables), and the industry import-export value (IEX) (from BEA's industry input-output use tables) as related instruments (Xue et al. 2012). The industry variables are weighted by a firm's sales in that industry. To estimate the firm's previous year's IT investment, we utilize the CI database. While these sets of instruments are most relevant to generic IT investments, we included the Hausman-type industry- averages of PECIs, TR, and their interaction as additional

instruments to improve the relevance of the set of instruments, following the existing literature (Aral et al. 2017; Cachon et al. 2018; Lu et al. 2017; Mithas and Rust 2016).

Moreover, to bolster the exogeneity conditions of our instruments, we focus on two exogenous shocks that can impact both a firm's PECIs and TR. First, and focusing on the legislative environment, we expect that the passage of legislation that requires investment in cybersecurity can be a suitable exogenous shock influencing both PECIs and TR. In looking for such legislation, we searched for those that show enough variation for the firms in our sample in the period of 2005 to 2015. Specifically, state laws passed to require firms to provide security breach notifications to stakeholders in case of cybersecurity breaches show relevance and variability in our sample. Between 2005 and 2015, all but three states (New Mexico, South Dakota, and Alabama), passed a version of security breach notification laws (SBNL), while California had passed its SBNL in 2002. Therefore, we used the passage of $SBNL_{it}$ as an additional instrument ($SBNL_{it}$= 1, if a version of SBNL law is passed[14] in the state where the headquarters of firm i is located, in year t or prior; $SBNL_{it}$= 0, otherwise).

Second, and focusing on local markets supplying cybersecurity knowledge and talent to a firm, we expect that the introduction of cybersecurity degrees in higher education institutions in metropolitan areas where a firm has customer-facing operations (or headquarters) can increase the access to cybersecurity talent and influence investment in cybersecurity. We mined our dataset of online resumes to identify emerging educational degrees related to cybersecurity (e.g., an undergraduate minor in information assurance, a master's degree in cybersecurity and risk management) in different metropolitan areas in the US. In sum, we identified 146 cybersecurity-related degrees, which began showing up in individuals' resumes from 2005 to 2015. We used the earliest graduation year for an emerging degree in the 2005-2015 window as the date from which the cybersecurity workforce educated with that degree enters the job market. Therefore, the second

[14] We use the date that law is signed for our analysis, as it is the point of time in which firms absorb the legislative news and start reacting. However, models that consider the effective date for the law for measuring SBNL variable produce qualitatively similar results. These results are available by authors upon request.

exogenous shock used as an instrument is the emergence of a cybersecurity degree ($CyberDeg_{it}$) in one of the metropolitan areas of operation to the firm ($CyberDeg_{it}$= 1, if a cybersecurity degree is started in at least one metropolitan area where firm i has some operations (in the form a customer-facing business unit or headquarters) in year t or prior; $CyberDeg_{it}$= 0, otherwise).

The set of these instruments show strong statistical relevance to the endogenous variables as shown in stage 1 estimations presented in Appendix B. Specifically, the Cragg-Donald Wald F Statistic exceeds 5% maximal bias of the IV estimator relative to OLS in all four subsamples and in both equations (Stock and Yogo 2005), rejecting the null hypothesis of the equations being weakly identified (For Equation (1): SS1's F-statistic = 3282.16, SS2's F-statistic = 2443.89, SS3's F-statistic = 3517.74, SS4's F-statistic = 2438.46, Stock and Yogo's critical value for 2 endogenous variables and 12 instruments= 19.40; For Equation (2): SS1's F-statistic = 2812.12, SS2's F-statistic = 3008.93, SS3's F-statistic = 3192.32, SS4's F-statistic = 2457.22, Stock and Yogo's critical value for 3 endogenous variables and 12 instruments= 17.80). Moreover, the Sargan's test of over-identification fails to reject the null hypothesis that the set of instruments used in Equations (1) and (2) are exogenous to error terms (For Equation (1): p = 0.417 for SS1, p = 0.338 for SS2, p = 0.572 for SS3, p = 0.403 for SS4; For Equation (2): p = 0.392 for SS1, p = 0.217 for SS2, p = 0.187 for SS3, p = 0.282 for SS4).

2.4 Results

We start by a set of preliminary analyses to ensure the validity of our estimation and sampling approach. These analyses are then followed by a set of analyses that provide evidence pertaining to the business value of PECIs. Then, these main analyses are supplemented by a set of tests that shed light on the possible mechanisms through which business value is created by PECIs.

2.4.1 Preliminary results

We preface our analysis by providing estimations of equation 2 for the full unrestricted (I) and the matched samples (A), both using a regular fixed-effects estimation and a panel 2SLS regression. We

conduct this preliminary analysis to present the potential upward bias that may occur if an unrestricted sample is used to conduct our main analyses. Table 2.4 presents the result of these preliminary estimations. Columns 1 and 2 in Table 2.4 provide estimates from the unrestricted sample (I), and columns 3 and 4 provide the results of the estimation in the matched sample (A). The coefficients of $PECI$, TR, and $TR \times PECI$ are significant and positive across the four estimations. However, the effect sizes are considerably larger in the unrestricted samples as compared to the matched sample estimates. The inflated estimates in the unrestricted sample may indicate an upward bias when treated observations are compared to a set of uncontrolled counterfactuals. Therefore, to increase the validity of our hypothesis testing, we present our main analyses in the four subsamples based on estimates in the matched sample (A), which provides more conservative estimates.

Table 2.4 Preliminary Results

	FE **Unrestricted sample (I)** (1)	**2SLS** **Unrestricted sample (I)** (2)	**FE** **Matched sample (A)** (3)	**2SLS** **Matched sample (A)** (4)
PECIs (H1)	**0.092*** (0.008)**	**0.064* (0.030)**	**0.043*** (0.007)**	**0.033* (0.017)**
TR	0.114*** (0.003)	0.081* (0.04)	0.058* (0.028)	0.051* (0.024)
TR×PECIs (H2)	**0.103*** (0.007)**	**0.059* (0.027)**	**0.041** (0.015)**	**0.032* (0.013)**
Firm size	0.038*** (0.007)	0.021# (0.012)	0.017** (0.007)	0.019# (0.011)
Assets	0.196*** (0.015)	0.073* (0.03)	0.062* (0.031)	0.055* (0.022)
Diversification	0.006 (0.004)	0.005 (0.003)	0.004 (0.003)	0.004 (0.003)
R&D	0.208*** (0.003)	0.172** (0.056)	0.111*** (0.029)	0.092*** (0.015)
ADV	0.343*** (0.009)	0.205** (0.066)	0.192*** (0.049)	0.081*** (0.013)
Firm FE	Yes	Yes	Yes	Yes
Year FE	Yes	Yes	Yes	Yes
Wald's Chi	14232.417	9873.209	5008.928	2812.372
Observations	*99904*	*99904*	*3130*	*3130*

Notes. *In coloumn 3 and 4, each observation is paired with at least one observation in an adjacent year without an announcement. PECIs stands for publicly emphasizing cybersecurity investments, TR for talent recruitment, and ADV for advertising expenditure. Standard errors are in parentheses. ***p < 0.001; **p < 0.01; *p < 0.05; # p < 0.10.*

2.4.2 Main results

Table 2.5 presents our main analysis. From panel A in Table 5, evidence regarding H1 and H2 is obtained. The coefficients of PECIs are positive and significant across all subsamples (supporting H1). The coefficients of the interaction term with talent recruitment (TR×PECIs) are also significantly positive for all subsample (supporting H2). Panel B provides evidence regarding subsample comparison hypotheses (H3 and H4). Comparisons in the $PECIs$ submatrix, included in

panel B, suggest that direct effect sizes are significantly larger for SS1 compared to SS2. Also, the coefficient in SS4 is higher significantly relative to SS2 and SS3 (supporting H3). Moreover, the interaction effect sizes, reported in $TR \times PECIs$ submatrix of the panel B, show that the coefficient estimates are significantly larger for both SS1 and SS4 relative to SS2 and SS3 (supporting H4). It is also worth noting that given the impact of PECI is complemented by the level of TR it is more appropriate to conduct an analysis that compares the effect size of $PECIs + TR + TR \times PECIs$, across the four subsamples. This analysis compares the impact of PECIs across the subsamples under a high value for TR. Results in the $PECIs + TR + TR \times PECIs$ submatrix of Panel B in Table 5 show that firms in SS1 and SS4 gain significantly higher payoffs. Taken together, the results suggest that while PECIs generally increase a firm's Tobin's q, the impact is specifically stronger for firms that have under- or over-performed relative to other firms in their industry. Moreover, we note that terms pertaining to PECIs in the absence of TR (η_{it}) are only significantly positive for SS1 and SS4. This finding suggests that PECIs in absence of recruited talent can be met with economic benefits, but only for under- and over-performing firms where investors may be excessively sensitive to the publicly-announced initiatives.

The results show that PECIs produce higher market rewards when a firm has substantive support for them through talent recruitment. Ceteris paribus, a firm that has one standard deviation higher than average PECIs benefits form a 5 percent higher market to book value. Moreover, a firm that has a high PECIs and successfully recruits cybersecurity talent, at one standard deviation above what an average firm can recruit, can add to its market to book value gains as a result of a high PECIs by an average of 6 percent and as high as 13 percent (for over-performers).

While the main analyses provide evidence of the positive business value of PECIs as well as value heterogeneity across the subsamples as measured by Tobin's q, we further investigate if the positive value is still detectable using traditional book-keeping measures of performance, i.e., return on assets (ROA) and return on sales (ROS). We run models like those in Table 2.5 with ROA/ROS as

dependent variables both contemporaneously, as well as with one and two-year lags. We could only explore lags as deep as two because ROA could be calculated for up to 2017 for the observations in 2015. While contemporaneous and 1-year lagged models did not detect the impacts of PECIs or TR, the 2-year lagged models, presented in Tables 2.6 and 2.7, show similar patterns as observed in Table 2.5. Hence, the positive business value estimated by a forward-looking measure such as Tobin's *q* can be traced in the book-keeping measures with a deep enough lag. It suggests that early market rewards for PECIs and talent recruitment transpire in accounting measures of success a few years down the line.

Table 2.5 Panel A: Main results

2SLS + Matching	**SS1: Under-performing firms**		**SS2: On-par firms (high risk)**		**SS3: On-par firms (low risk)**		**SS4: Over-performing firms**	
DV=Tobin's q	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
PECIs (H1)	**0.044***	**0.057***	**0.014#**	**0.015#**	**0.021***	**0.039***	**0.054***	**0.064***
	(0.021)	**(0.024)**	**(0.007)**	**(0.008)**	**(0.009)**	**(0.019)**	**(0.025)**	**(0.029)**
TR	0.075*	0.134***	0.035*	0.029*	0.014#	0.016#	0.065*	0.095***
	(0.03)	(0.031)	(0.017)	(0.014)	(0.007)	(0.009)	(0.028)	(0.02)
TR×PECIs (H2)		**0.057***		**0.012#**		**0.016#**		**0.081****
		(0.027)		**(0.007)**		**(0.009)**		**(0.025)**
Firm size	0.015#	0.023*	0.007	0.004	0.009	0.014#	0.024*	0.024*
	(0.008)	(0.01)	(0.004)	(0.003)	(0.006)	(0.008)	(0.009)	(0.01)
Assets	0.072*	0.072*	0.072*	0.049*	0.039*	0.04*	0.034*	0.041*
	(0.029)	(0.032)	(0.031)	(0.024)	(0.017)	(0.02)	(0.014)	(0.016)
Diversification	-0.011	-0.010	0.000	0.000	0.000	0.000	-0.011	-0.010
	(0.007)	(0.008)	(0.003)	(0)	(0)	(0.004)	(0.009)	(0.008)
R&D	0.224***	0.202***	0.064*	0.111***	0.068*	0.07*	0.261***	0.142***
	(0.036)	(0.033)	(0.027)	(0.029)	(0.03)	(0.028)	(0.045)	(0.036)
ADV	0.158***	0.214***	0.121***	0.174***	0.203***	0.178***	0.083**	0.059*
	(0.03)	(0.053)	(0.021)	(0.027)	(0.031)	(0.043)	(0.027)	(0.025)
Firm FE	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Year FE	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Wald's Chi	4911.540	2305.470	2286.900	3966.560	1887.930	883.503	1634.880	1757.600
Observations	*884*		*718*		*922*		*606*	

Notes. *Each observation is paired with at least one observation in an adjacent year without an announcement. PECIs stands for publicly emphasizing cybersecurity investments, TR for talent recruitment, ADV for advertising expenditure. ***p < 0.001; **p < 0.01; *p < 0.05; # p < 0.10.*

Panel B: Coefficient comparisons among subsamples

	PECIs (H3)			**TR×PECIs (H4)**			PECIs+TR+TR×PECIs		
	SS1	SS2	SS3	SS1	SS2	SS3	SS1	SS2	SS3
SS2	**0.062**			**0.084**			**0.005**		
SS3	**0.081**	**0.683**		**0.054**	**0.962**		**0.002**	**0.854**	
SS4	**0.522**	**0.091**	**0.089**	0.057	**0.000**	**0.000**	**0.574**	**0.000**	**0.000**

Notes. *The reported numbers are p-values for Chi-squared tests (based on standard errors estimated from simultaneous equations in a GMM recasting of 2SLS) for coefficient differences in column 2, 4, 6, 8 of Panel A. SS1-SS2, SS1-SS3, SS4-SS2, SS4-SS3 are one-tailed (expect p<0.1), SS1-SS4, SS2-SS3 are two-tailed (expect p≥0.1). Results consistent with expectations are boldfaced.*

Table 2.6 Panel A: Robustness tests with ROA

2SLS + Matching	**SS1: Under-performing firms**		**SS2: On-par firms (high risk)**		**SS3: On-par firms (low risk)**		**SS4: Over-performing firms**	
DV=ROA	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
PECIs (H1)	**0.04***	**0.036***	**0.012#**	**0.021***	**0.034***	**0.042***	**0.057***	**0.043***
	(0.02)	**(0.018)**	**(0.006)**	**(0.009)**	**(0.015)**	**(0.021)**	**(0.022)**	**(0.017)**
TR	0.105***	0.096***	0.043*	0.038*	0.018#	0.021*	0.103***	0.114***
	(0.023)	(0.015)	(0.018)	(0.017)	(0.01)	(0.008)	(0.016)	(0.024)
TR×PECIs (H2)		**0.067***		**0.009**		**0.008**		**0.119*****
		(0.034)		**(0.007)**		**(0.006)**		**(0.035)**
Firm size	0.015#	0.013#	0.006	0.004	0.009	0.017#	0.024*	0.018#
	(0.008)	(0.007)	(0.004)	(0.002)	(0.006)	(0.009)	(0.011)	(0.01)
Assets	0.067*	0.056*	0.043*	0.061*	0.033*	0.061*	0.016#	0.049*
	(0.03)	(0.026)	(0.019)	(0.024)	(0.015)	(0.031)	(0.008)	(0.022)
Diversification	0.000	0.000	0.000	0.000	-0.009	-0.010	0.000	0.000
	(0.005)	(0.003)	(0.004)	(0.003)	(0.008)	(0.006)	(0.002)	(0.003)
R&D	0.226***	0.155***	0.073*	0.107***	0.127***	0.126***	0.165***	0.162***
	(0.068)	(0.036)	(0.032)	(0.026)	(0.032)	(0.036)	(0.03)	(0.026)
ADV	0.239***	0.153***	0.143***	0.273***	0.177***	0.133***	0.043*	0.076*
	(0.065)	(0.03)	(0.024)	(0.045)	(0.043)	(0.038)	(0.019)	(0.035)
Firm FE	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Year FE	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Wald's Chi	1290.100	1893.840	825.884	1536.900	1482.030	1450.650	657.195	1469.820
Observations	*884*		*718*		*922*		*606*	

Notes. *Each observation is paired with at least one observation in an adjacent year without an announcement. PECIs stands for publicly emphasizing cybersecurity investments, TR for talent recruitment, ADV for advertising expenditure. ***p < 0.001; **p < 0.01; *p < 0.05; #p < 0.10.*

Panel B: Coefficient comparisons among subsamples

	PECIs (H3)			**TR×PECIs (H4)**			PECIs+TR+TR×PECIs		
	SS1	SS2	SS3	SS1	SS2	SS3	SS1	SS2	SS3
SS2	**0.078**			0.105			**0.006**		
SS3	0.103	**0.867**		**0.071**	**0.933**		**0.002**	**1.110**	
SS4	**0.637**	0.114	0.109	0.074	**0.000**	**0.000**	**0.677**	**0.000**	**0.000**

Notes. *The reported numbers are p-values for Chi-squared tests (based on standard errors estimated from simultaneous equations in a GMM recasting of 2SLS) for coefficient differences in column 2, 4, 6, 8 of Panel A. SS1-SS2, SS1-SS3, SS4-SS2, SS4-SS3 are one-tailed (expect p<0.1), SS1-SS4, SS2-SS3 are two-tailed (expect p≥0.1). Results consistent with expectations are boldfaced.*

Table 2.7 Panel A: Robustness tests with ROS

2SLS + Matching	**SS1: Under-performing firms**		**SS2: On-par firms (high risk)**		**SS3: On-par firms (low risk)**		**SS4: Over-performing firms**	
DV=ROS	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
PECIs (H1)	**0.025***	**0.061***	**0.012#**	**0.018#**	**0.023***	**0.044***	**0.041***	**0.071***
	(0.011)	**(0.029)**	**(0.007)**	**(0.01)**	**(0.011)**	**(0.018)**	**(0.018)**	**(0.029)**
TR	0.072*	0.136***	0.04*	0.035*	0.013#	0.023*	0.063*	0.11***
	(0.035)	(0.032)	(0.016)	(0.015)	(0.007)	(0.011)	(0.026)	(0.017)
TR×PECIs (H2)		**0.052***		**0.009**		**0.012#**		**0.094*****
		(0.023)		**(0.006)**		**(0.007)**		**(0.022)**
Firm size	0.015#	0.02*	0.006	0.005	0.011	0.015#	0.03*	0.022*
	(0.008)	(0.009)	(0.005)	(0.003)	(0.007)	(0.008)	(0.013)	(0.009)
Assets	0.076*	0.066*	0.05*	0.071*	0.046*	0.051*	0.019#	0.053*
	(0.034)	(0.028)	(0.021)	(0.031)	(0.023)	(0.02)	(0.011)	(0.021)
Diversification	0.000	0.000	0.000	0.000	0.000	0.000	-0.009	-0.010
	(0.001)	(0.003)	(0.002)	(0.005)	(0.002)	(0.002)	(0.007)	(0.007)
R&D	0.258***	0.211***	0.052*	0.104***	0.105***	0.13***	0.174***	0.145***
	(0.058)	(0.046)	(0.02)	(0.031)	(0.03)	(0.02)	(0.029)	(0.025)
ADV	0.169***	0.158***	0.169***	0.228***	0.141***	0.118***	0.05*	0.08**
	(0.046)	(0.032)	(0.033)	(0.04)	(0.022)	(0.018)	(0.022)	(0.028)
Firm FE	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Year FE	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Wald's Chi	1324.230	1355.740	1301.120	1281.320	1288.720	1293.600	606.424	1870.360
Observations	*884*		*718*		*922*		*606*	

Notes. *Each observation is paired with at least one observation in an adjacent year without an announcement. PECIs stands for publicly emphasizing cybersecurity investments, TR for talent recruitment, ADV for advertising expenditure. ***p < 0.001; **p < 0.01; *p < 0.05; #p < 0.10.*

Panel B: Coefficient comparisons among subsamples

	PECIs (H3)			**TR×PECIs (H4)**			PECIs+TR+TR×PECIs		
	SS1	SS2	SS3	SS1	SS2	SS3	SS1	SS2	SS3
SS2	**0.075**			0.110			**0.006**		
SS3	**0.104**	**0.826**		**0.069**	**1.203**		**0.003**	**1.068**	
SS4	**0.626**	**0.098**	0.112	0.073	**0.000**	**0.000**	**0.746**	**0.000**	**0.000**

Notes. *The reported numbers are p-values for Chi-squared tests (based on standard errors estimated from simultaneous equations in a GMM recasting of 2SLS) for coefficient differences in column 2, 4, 6, 8 of Panel A. SS1-SS2, SS1-SS3, SS4-SS2, SS4-SS3 are one-tailed (expect p<0.1), SS1-SS4, SS2-SS3 are two-tailed (expect p≥0.1). Results consistent with expectations are boldfaced.*

2.4.3 The value-creation mechanism

In our theoretical discussions, we explained that we expect cybersecurity investments, broadcasted in SEC filings, and supported by cybersecurity talent recruitment, create value through reducing the cybersecurity risks, and thereby reducing the average cost of capital. While our main analyses provide empirical evidence that suggests PECIs and TR interact to create value (both in forward-looking and book-keeping measures of business value), it is imperative to provide empirical evidence that sheds light on the value-creating mechanism. Therefore, to further unfold the impact of

cybersecurity investments on subsequent security risks, we explore their security implications by replacing the dependent variable in Table 5 with the occurrence of a security breach in the subsequent year[15]. We note that while PECIs and TR×PECIs have a significant negative effect towards breaches across all subsamples, PECIs in absence of TR do not have any significant effect towards breaches (Table 2.7). Moreover, we estimated equation (3) while replacing the dependent variable with the cost of capital (Table 2.8), following Sharfman and Fernando's (2008) measure of the weighted average cost of capital (WACC), which considers the general case of a firm with both equity and debt financing[16]. While R&D consistently reduces WACC across all subsamples, the results show that the coefficients of PECIs, TR, and PECIs×TR significantly and negatively impact WACC only in SS1 and SS4, but not in SS2 and SS3.

Although this analysis suggests that PECIs and TR reduce the cost of capital, it is imperative to rule out other outstanding sources of the cost that can also be cut due to PECIs. Otherwise, it may not be clear if the observed impacts on the reduction of cost of capital are due to the stakeholders' re-evaluation of the broader risks (e.g., long-term reputational risks), or simply due to a reduction in the firm's operational costs. Specifically, since cybersecurity breaches disrupt a firm's operations and increase its overhead costs, pursuing cybersecurity investments may also reduce the cost of goods sold. Table 9 presents the results when the cost of goods sold is considered as the dependent variable in estimating equation (3). While the results show that firms with more assets and higher R&D expenditure generally benefit from a lower cost of goods sold, PECIs and TR do not show any significant impact. This non-finding is aligned with the existing literature on cybersecurity breaches, suggesting that the operational costs of an incident disruption are only a part of the broader set of costs pertaining to reputation loss and the remediating strategic shifts (Kvochko and Pant 2015), and firms with enough slack resources can usually bounce back from operational damages. However, the

[15] A Cox proportional hazard estimation with stratification around firm id (i.e., distinct baseline hazard for each firm) and a robust standard error estimation are used. The exit condition is set to happen until the next observation about the same firm in another year or the end of the study.

[16] See Appendix C for the full formula used in estimating WACC.

long-term reputational impacts, or at least a negative outlook, may be harder to overcome with slack resources and financial cushions. Since cost of capital determined by stakeholders considers both the broader legitimacy impacts of cybersecurity incidents (and thereby, the preventive impact of PECIs) and the immediate operational efficiencies (Sharfman and Fernando 2008), the positive and significant impact of PECIs and TR on cost of capital, but not on cost of goods sold (see SS1 and SS4 in Table 9) suggests that these broader legitimacy impacts are the likely reasons for observing the reduction in the cost of capital.

Table 2.8 Panel A: The hazard of a future breach

2SLS + Matching	**SS1: Under-performing firms**		**SS2: On-par firms (high risk)**		**SS3: On-par firms (low risk)**		**SS4: Over-performing firms**	
DV=security hazard	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
PECIs (H1)	**-0.011#**	**-0.043***	**-0.011**	**0.000**	**0.000**	**0.000**	**-0.02***	**-0.062***
	(0.006)	**(0.019)**	**(0.008)**	**(0.002)**	**(0.004)**	**(0.004)**	**(0.009)**	**(0.028)**
TR	-0.1***	-0.071*	-0.02*	-0.010	0.000	-0.02*	-0.072*	-0.056*
	(0.016)	(0.032)	(0.009)	(0.006)	(0.001)	(0.01)	(0.034)	(0.026)
TR×PECIs (H2)		**-0.078****		**-0.010**		**-0.011**		**-0.099*****
		(0.026)		**(0.007)**		**(0.007)**		**(0.021)**
Firm size	-0.010	-0.011	-0.021*	0.000	0.000	-0.022*	-0.010	-0.010
	(0.007)	(0.008)	(0.01)	(0.004)	(0.003)	(0.01)	(0.008)	(0.008)
Assets	0.008	0.007	0.005	0.006	0.006	0.006	0.011	0.005
	(0.005)	(0.005)	(0.004)	(0.004)	(0.004)	(0.005)	(0.008)	(0.004)
Diversification	-0.009	-0.009	0.000	-0.010	0.000	-0.011	0.000	-0.010
	(0.008)	(0.006)	(0.001)	(0.006)	(0.002)	(0.009)	(0.003)	(0.007)
R&D	-0.036*	-0.074*	-0.039*	-0.045*	-0.097***	-0.091**	-0.077*	-0.086**
	(0.014)	(0.034)	(0.017)	(0.018)	(0.018)	(0.029)	(0.033)	(0.029)
ADV	0.006	0.004	0.004	0.004	0.005	0.004	0.005	0.010
	(0.004)	(0.003)	(0.003)	(0.004)	(0.003)	(0.003)	(0.004)	(0.008)
Firm FE	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Year FE	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Wald's Chi	1327.200	1879.380	1252.710	1337.220	982.560	1256.310	434.250	1602.420
Observations	*884*		*718*		*922*		*606*	

Notes. *Each observation is paired with at least one observation in an adjacent year without an announcement. PECIs stands for publicly emphasizing cybersecurity investments, TR for talent recruitment, ADV for advertising expenditure. ***p < 0.001; **p < 0.01; *p < 0.05; #p < 0.10.*

Panel B: Coefficient comparisons among subsamples

	PECIs (H3)			**TR×PECIs (H4)**			PECIs+TR+TR×PECIs		
	SS1	SS2	SS3	SS1	SS2	SS3	SS1	SS2	SS3
SS2	**0.012**			**0.004**			**0.000**		
SS3	**0.013**	**0.817**		**0.001**	**0.350**		**0.000**	**0.581**	
SS4	**0.979**	**0.021**	**0.020**	**0.875**	**0.001**	**0.001**	**0.965**	**0.000**	**0.000**

Notes. *The reported numbers are p-values for Chi-squared tests (based on standard errors estimated from simultaneous equations in a GMM recasting of 2SLS) for coefficient differences in column 2, 4, 6, 8 of Panel A. SS1-SS2, SS1-SS3, SS4-SS2, SS4-SS3 are one-tailed (expect p<0.1), SS1-SS4, SS2-SS3 are two-tailed (expect p≥0.1). Results consistent with expectations are boldfaced.*

Table 2.9 Panel A: Cost of capital

2SLS + Matching	**SS1: Under-performing firms**		**SS2: On-par firms (high risk)**		**SS3: On-par firms (low risk)**		**SS4: Over-performing firms**	
DV=cost of capital	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
PECIs (H1)	**-0.013#**	**-0.032***	**0.000**	**0.000**	**0.000**	**0.000**	**-0.010**	**-0.036***
	(0.007)	**(0.016)**	**(0.001)**	**(0.002)**	**(0.004)**	**(0.002)**	**(0.007)**	**(0.014)**
TR	-0.077*	-0.067*	-0.022*	-0.007	0.000	-0.023	-0.064*	-0.073*
	(0.03)	(0.03)	(0.01)	(0.005)	(0.003)	(0.02)	(0.027)	(0.03)
TR×PECIs (H2)		**-0.074***		**-0.008**		**0.000**		**-0.091****
		(0.032)		**(0.005)**		**(0.003)**		**(0.028)**
Firm size	0.000	-0.007	-0.021*	0.000	0.000	-0.010	0.000	0.000
	(0.001)	(0.005)	(0.01)	(0.001)	(0.001)	(0.006)	(0.002)	(0.003)
Assets	0.008	0.006	0.005	0.005	0.005	0.007	0.011	0.005
	(0.005)	(0.005)	(0.004)	(0.003)	(0.004)	(0.005)	(0.007)	(0.003)
Diversification	-0.013#	-0.008	0.000	0.000	0.000	-0.010	0.000	0.000
	(0.007)	(0.007)	(0.001)	(0.002)	(0.004)	(0.009)	(0.004)	(0.001)
R&D	-0.039*	-0.046*	-0.038*	-0.037*	-0.119***	-0.097***	-0.067*	-0.086**
	(0.017)	(0.021)	(0.017)	(0.016)	(0.027)	(0.018)	(0.031)	(0.027)
ADV	0.004	0.005	0.005	0.004	0.005	0.004	0.005	0.009
	(0.003)	(0.004)	(0.003)	(0.003)	(0.003)	(0.003)	(0.004)	(0.006)
Firm FE	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Year FE	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Wald's Chi	1102.890	1822.690	1076.400	905.760	983.550	725.400	421.512	1848.960
Observations	*884*		*718*		*922*		*606*	

Notes. *Each observation is paired with at least one observation in an adjacent year without an announcement. PECIs stands for publicly emphasizing cybersecurity investments, TR for talent recruitment, ADV for advertising expenditure. ***p < 0.001; **p < 0.01; *p < 0.05; #p < 0.10.*

Panel B: Coefficient comparisons among subsamples

	PECIs (H3)			**TR×PECIs (H4)**			PECIs+TR+TR×PECIs		
	SS1	SS2	SS3	SS1	SS2	SS3	SS1	SS2	SS3
SS2	**0.022**			**0.068**			**0.000**		
SS3	**0.014**	**0.350**		**0.016**	**0.121**		**0.000**	0.033	
SS4	**0.950**	**0.015**	**0.008**	**0.475**	**0.003**	**0.003**	**0.159**	**0.000**	**0.000**

Notes. *The reported numbers are p-values for Chi-squared tests (based on standard errors estimated from simultaneous equations in a GMM recasting of 2SLS) for coefficient differences in column 2, 4, 6, 8 of Panel A. SS1-SS2, SS1-SS3, SS4-SS2, SS4-SS3 are one-tailed (expect p<0.1), SS1-SS4, SS2-SS3 are two-tailed (expect p≥0.1). Results consistent with expectations are boldfaced.*

Table 2.10 Cost of goods sold

2SLS + Matching	**SS1: Under-performing firms**		**SS2: On-par firms (high risk)**		**SS3: On-par firms (low risk)**		**SS4: Over-performing firms**	
DV=COGS	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
PECIs (H1)	**0.007**	**0.008**	**0.006**	**0.008**	**0.005**	**0.005**	**0.004**	**0.004**
	(0.006)	**(0.006)**	**(0.005)**	**(0.005)**	**(0.003)**	**(0.003)**	**(0.003)**	**(0.002)**
TR	0.010	0.007	0.008	0.009	0.008	0.010	0.008	0.006
	(0.007)	(0.006)	(0.006)	(0.005)	(0.006)	(0.006)	(0.006)	(0.004)
TR×PECIs (H2)		**0.000**		**0.000**		**0.000**		**0.000**
		(0.004)		**(0.001)**		**(0.002)**		**(0.001)**
Firm size	-0.009	-0.009	0.000	-0.009	0.000	-0.010	0.000	-0.011
	(0.007)	(0.006)	(0.003)	(0.007)	(0.004)	(0.006)	(0.004)	(0.007)
Assets	-0.045*	-0.056*	-0.04*	-0.056*	-0.045*	-0.035*	-0.041*	-0.031*
	(0.023)	(0.026)	(0.018)	(0.029)	(0.022)	(0.016)	(0.02)	(0.014)
Diversification	-0.009	-0.009	0.000	-0.009	0.000	-0.010	0.000	-0.011
	(0.005)	(0.007)	(0.001)	(0.005)	(0.004)	(0.009)	(0.001)	(0.007)
R&D	-0.042*	-0.078**	-0.041*	-0.051*	-0.099***	-0.104***	-0.076*	-0.086**
	(0.019)	(0.027)	(0.017)	(0.022)	(0.022)	(0.03)	(0.031)	(0.032)
ADV	0.006	0.004	0.004	0.004	0.005	0.004	0.005	0.009
	(0.005)	(0.003)	(0.003)	(0.003)	(0.004)	(0.003)	(0.004)	(0.005)
Firm FE	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Year FE	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Wald's Chi	1102.050	1808.460	1185.360	1193.010	1185.480	1142.100	439.075	1633.840
Observations	*884*		*718*		*922*		*606*	

Notes. *Each observation is paired with at least one observation in an adjacent year without an announcement. PECIs stands for publicly emphasizing cybersecurity investments, TR for talent recruitment, ADV for advertising expenditure. ***p < 0.001; **p < 0.01; *p < 0.05; #p < 0.10.*

2.5 Discussion

Cybersecurity has transformed from its once operational nature in the organization and turned into a key strategic area of focus. With such a transformation in its organizational meaning, the organizational inquiry about cybersecurity has also transformed: from a focus on its immediate impacts on cyber-risk reduction to the broader business, value-creating impacts. Specifically, while the preventive value of cybersecurity investments is well established and evidence exists pertaining to its business value, at least in a short window of reaction or relative to a limited set of investments, the enigma lies in connecting the dots between being protected and gaining economic rents that prevail. To unfold the enigma, we build on organizational theories that connect protection against risks to sources of profit and economic gains. We wear a legitimacy lens to view a public firm as an organism that survives with reputation, depends on trust, and breathes with critical financial leverage. In such a view, measures taken to reduce outstanding risks or remediate outstanding damages are not only

rewarded by operational efficiency, but also are met with an enhanced reputation, increased trust, and subsequently, cheaper access to debt and equity finances. The collection of our findings paints a picture of cybersecurity investments that: a) connects them to the book-keeping indices of sustained performance, b) ties them into the deeper strategic efforts of talent acquisition in competitive markets, c) makes them relevant to the institutional positioning of a firm relative to its peers, and d) positions them in a significant role in connecting to stakeholders and accessing competitive sources of financing. Together, these findings provide further clarity regarding the strategic transformation of cybersecurity in organizations.

This study is not without its *limitations*. First, our dataset on PECI is limited to those that are publicly available. While this fits with our focus on the stakeholders' reactions, some cybersecurity investments may not be announced to protect the integrity of the initiatives. Second, security breaches, in general, tend to be under-reported (Amir et al. 2018) since managers are incentivized to withhold potentially damaging information from the public, and such under-reporting may bias the estimates. Third, our examination of the lagged impact on book-keeping measures of performance is limited to only two years due to the short and unbalanced nature of the panel. We acknowledge that the long-term impacts of cybersecurity investments require further empirical scrutiny in future research. Despite its limitations, this paper has a few important *contributions*.

First, this study reveals and quantifies the complementary role of security expertise in creating value from cybersecurity investments. Prior literature has pointed out the essential role of substantive adoption of security technology in mitigating security threats (Angst et al. 2017; Kwon and Johnson 2018). We extend this literature, which has identified *general institutional* characteristics, such as size and entrepreneurship orientation, influencing the substantiveness of cybersecurity investments, by introducing and empirically evaluating the role of one critical *cyber-specific* characteristics, i.e., cybersecurity talent. This finding ties this stream of research in cybersecurity to the general literature on BVIT that has highlighted the *direct* value of IT labor (e.g., Tambe 2014) and provides empirical evidence showcasing its *complementary* role in increasing value reaped from ongoing organizational

investments and initiatives. This integration is more critical in a salient context such as cybersecurity where there is a significant talent shortage.

Second, this study offers a framework to explain the value heterogeneity of publicly emphasized cybersecurity investments by showing why some public emphases are more valuable for over- and under-performing firms than for those that are performing as expected in terms of their relative vulnerabilities. Building on the literature related to organizational legitimacy and BTOF, as well as the literature outlining security breach motives (Cremonini and Nizovtsev 2009), the study shows that the valuation of cybersecurity investments not only depends on the firm itself but also on the relative stance of the firm while considering industry benchmarks. While the social comparison account has recently been utilized in studying the BVIT literature (Ho et al. 2017), we extend its use to understanding the value of publicly emphasizing information security investments. The study offers a framework to build industry benchmarks when the assessment of cybersecurity investments is concerned. In addition to its theoretical implications, the study examines a sample which spans a wide variety of cybersecurity investments in different industries, adding to the rich knowledge accumulated in VCI studies that either focus on a specific type of cybersecurity investment (e.g., Bose and Leung 2019) or a particular industry (e.g., Angst et al. 2017).

Finally, and most importantly, the study extends the work on the business and preventive value of publicly emphasized cybersecurity investments (e.g., Gordon et al. 2010; Angst et al. 2017) by theoretically discussing and empirically unfolding an important mechanism that can explain how the preventive value of cybersecurity turns into business value. Building on the legitimacy view, which positions stakeholders in central roles both in assessing the firm's legitimacy and in regulating the costs of its access to capital, we show that patterns of reducing cybersecurity hazard through PECIs and TR are matched when the impact of those factors on the firm's cost of capital is considered. Therefore, our study recognizes the risk-reducing nature of cybersecurity investments and builds on the general strategic management studies that had highlighted the value-creating path of other risk-reducing investments (e.g., Sharfman and Fernando 2008). In doing so, we establish an important link

between the preventive and business value of cybersecurity investments. Moreover, we unfold that the PECIs do not significantly impact the operational costs (i.e., cost of goods sold). While previous research on BVIT has highlight the role of general IT in reducing operational costs (Santhanam and Hartono 2003), this finding contrasts the cost-reduction nature of cybersecurity investments with that of general IT.

For practitioners, the finding pertaining to the impact of PECIs in reducing the firm's cost of capital, but not reducing the operational costs, changes the ways that executives incentivize and champion for cybersecurity investments. While a limited operational look at impacted costs may not capture the full effect of cybersecurity investments, focusing on the broader structure of costs of accessing debt and equity financing may provide a clearer picture. Further, since the market profitability of cybersecurity investments can also be traced in later values of traditional accounting indices, managers should allow enough time elapse before they scrutinize their firm's financial reports to quantify such benefits. Nonetheless, once enough time is elapsed, they can rely on more direct book-keeping evidence to appraise their current cybersecurity efforts and champion for future plans. The findings also highlight the importance of scrutinizing and enhancing recruitment policies that allow a firm to attract the hot and rare cybersecurity expertise, parallel with the public emphasizing of their cybersecurity investments. Further, this study has revealed an industry benchmark framework that can be used by top executives to evaluate the promise of PECIs and manage market reactions. The framework allows the championing executives to assess the firm's relative vulnerability in the underlying industry, and actively interpret the under-, over-, and on-par performance stance of the firm when incentivizing cyber initiatives.

CHAPTER III: CORPORATE VENTURE CAPITAL IN CYBERSECURITY[17]

3.1 Introduction

"So long as there are black hats, there will need to be white hats" (Pettit 2018). With the ever-increasing and costlier data breaches (Accenture 2017), entrepreneurship in cybersecurity is also booming (Peterson 2017; Peterson 2018; Pettit 2018), which attracted independent and corporate venture capitals alike. Unlike independent venture capitals that are purely profit-motivated, corporate investors are interested in cybersecurity startups for security sake. Gaining access to cutting-edge cybersecurity technologies could potentially save a company millions of dollars (Accenture 2017) and avoid public embarrassment as well as legal entanglements from data breaches. In addition, investing in an infant-stage blue-chip company could generate considerable future returns. On the other hand, shareholders may be skeptical towards such investments, since ventures in new-born companies may involve greater uncertainty relative to in-house R&D. Moreover, investment in cybersecurity is traditionally viewed as a cost of doing business rather than a profit-generating production factor (Kvochko and Pant 2015). As a mixture of security measures and corporate venture capital, organizational investment in cybersecurity startups can be profit-oriented or as a necessary cost element. Therefore, the business value of organizational investments in cybersecurity startups is unclear, and needs to be investigated empirically.

Studies of organizational investment in cybersecurity startups lie in the intersection of *cybersecurity investment* and *corporate venture capital* (CVC) literature. Researches on cybersecurity investment typically address disclosures of security-related initiatives (Chai et al. 2011; Gordon et al. 2010; Wang et al. 2013), and analytic assessments of cybersecurity

[17] We thank the participants at the 2018 Wharton Innovation Doctoral Symposium.

investment (Benaroch 2018; Cavusoglu et al. 2008; Wang et al. 2008). While direct investments in cybersecurity are generally associated with positive market reaction (Chai et al. 2011), it is not clear whether indirect cybersecurity investments through startups would generate similar outcomes. On the other hand, general CVC literature has documented the profitability of corporate investments in startups (Benson and Ziedonis 2009; Benson and Ziedonis 2010; Dushnitsky and Lenox 2006) and how value is transmitted from a startup to the investing firm (Chemmanur et al. 2014; Wadhwa and Kotha 2006). Recent CVC studies have covered emergent industries such as big data (Havakhor and Sabherwal 2018). CVC in cybersecurity is unique in the sense that cybersecurity capability is typically not regarded as a rent-seeking element (Kvochko and Pant 2015). In both streams of literature, the value of organizational investment in cybersecurity startup is understudied. To fill this void, this study investigates whether organizational investments in cybersecurity startups create business value for the investing firm (RQ).

This study adopts a theoretical lens that considers organizational investment in cybersecurity startups as a form of "real options", which provides the organization with future choices and potential for proprietary access to technology, expertise and monetary gains (McGrath et al. 2004). The real options reasoning is suitable for IT investments under uncertainty (Schwartz and Zozaya-Gorostiza 2003), particularly for technology positioning investment (McGrath 1997). With cybersecurity threats on the rise, corporations are better prepared for the future by purchasing "real options" to access cutting-edge cybersecurity technologies and expertise. Due to uncertainties in the cybersecurity realm, real options also provide alternatives for organizations that are not fully committed to acquiring novel technologies. Prior CVC literature has implicitly adopted the real options lens by suggesting that corporate investments in startups provide a window for the latest technologies (Benson and Ziedonis 2009). While abundant IT investment literature addressed real options pricing (Benaroch and Kauffman 2000; Herath and Herath 2008; Taudes et al. 2000), this study focuses on the market valuation of CVC investments in cybersecurity through the theoretical lens of real options.

Data on CVC funding in cybersecurity startups are gathered from Crunchbase, a database that tracks funding and acquisitions of startups. Cybersecurity startups were identified using the venture categories and keyword search in Crunchbase. The CVC investment data was augmented with the investing firms' performance data from Computstat and CRSP. The economic impacts of CVC investments in cybersecurity are examined through a sample of 873 firm-year observations spanning from 2009 to 2017. Data up to 2008 were discarded to minimize the effect of the financial crisis in the sample. The results indicate an overall positive effect of organizational investments in cybersecurity startups on the investing firms' Tobin's q. The effect is robust when tested using two conservative measures, return on assets and return on sales. In addition, the positive impact is stronger for IT firms and for investments made in recent years, where security breaches have become more prevalent and costlier (Accenture 2017).

This paper contributes to the economics of cybersecurity literature by providing evidence of profitability in indirect cybersecurity investments through startups, suggesting that the real options into future cybersecurity technology and expertise are valuable to organizational investors. The study also adds to the CVC literature by revealing the tangible value of organizational investments in non-rent-seeking technologies. For practitioners, this paper will shed light on how investors react towards organizations tapping into future cybersecurity technologies through CVC investments. The rest of the article is organized as follows. We first review relevant literature on CVC and real options, before developing hypotheses in §3.2. Data collection and analyses are presented in §3.3 and §3.4, respectively. Finally, we discuss the limitations and implications in §3.5.

3.2 Theory development

3.2.1 Corporate venture capital

Corporate venture capital (CVC) is an investment by an established firm in entrepreneurial ventures. CVC typically creates values for the investing companies through two channels. First, "direct financial benefits from CVC due to privileged knowledge in selecting valuable ventures and

the possession of complementary assets that enhance the value of their portfolio companies" (Dushnitsky and Lenox 2006). Second, CVC may offer a valuable window of new technology that potentially opens pathways for future opportunities (Benson and Ziedonis 2009; Dushnitsky and Lenox 2006). While a few million funding could make a difference for an infant-stage company, the amount is dwarfed in comparison with the financial capabilities of the investing firms. For this reason, corporate investments may be less concerned with short-term financial gains. Indeed, gaining a window on new technologies is a prominent motive for CVC investing (Benson and Ziedonis 2009), whereas a short-term focus on financial objectives may inhibit long-term strategic benefits from external innovations through CVC investments (Ernst et al. 2005).

Value creations of CVC for the investing firms are subject to various internal and external factors. Internally, strategically focused CVC investments will create greater value than financially focused CVC investments (Dushnitsky and Lenox 2006); stable CVC programs lead to better performance (Benson and Ziedonis 2009); the investors' absorptive capacities of startups positively affect the innovation rate and consequently value-creation of CVC (Dushnitsky and Lenox 2005a; Dushnitsky and Lenox 2005b); R&D expenditure plays a complementary role in value creations by CVC investments (Benson and Ziedonis 2009); corporate investors' technological knowledge diversity and involvement in startups enhance knowledge creation by CVC investments (Wadhwa and Kotha 2006). Externally, uncertain environments for CVC-backed ventures tend to benefit the startups (Park and Steensma 2012), and likely the investing firms as well through increased investment returns. In addition, uncertainties in investing firms' environment will moderate the relationships between CVC investments and market reactions (Havakhor and Sabherwal 2018). Together, these confounding factors will affect the value of CVC investments.

On top of structural deficiencies of general CVCs (Chesbrough 2000; Sykes 1986), the business value of cybersecurity CVCs, in particular, can be murky due to its unique characteristics. While CVC investments harnessing novel technologies are associated with positive firm performance (Dushnitsky and Lenox 2006), cybersecurity CVC, as a form of indirect cybersecurity investments,

seems closer to a necessary cost than a production factor (Kvochko and Pant 2015). In this regard, the profitability of cybersecurity CVC is questionable. On the other hand, cybersecurity CVC possesses certain attributes implying positive firm performance. Cybersecurity management is a knowledge-intensive activity (Belsis et al. 2005), and investing in cybersecurity startups is a fast way to potentially gain access to the latest cybersecurity technologies and expertise, which will help protect shareholders' value in the event of a cyber-threat. In addition, high uncertainties in the cybersecurity industry (Baker 2018) will be beneficial to CVC-backed startups (Park and Steensma 2012), which will, in turn, increase the profitability of CVC investments. With conflicting arguments supporting both profitability and non-profitability of cybersecurity CVC, we proceed with the real options lens to better capture the future value of cybersecurity technologies.

3.2.2 Real options

It has been suggested that uncertain investments should be viewed through a real options lens (Dixit and Pindyck 1994). Adapted from financial options, a *real option* is a right, but not the obligation, to obtain the benefits associated with some physical assets (Fichman 2004). As a type of experimentation under uncertainties, venture capital investments can be conceptualized through a real options lens (Kerr et al. 2014). In particular, CVC investments entail valuable real options by offering the investing organization choices to increase, decrease, or defer substantial investments (Tong and Li 2011). Real options has also been applied in cybersecurity investment, although the emphasis has been placed on option pricing analytics (Benaroch 2018; Gordon et al. 2003; Herath and Herath 2008). We adopt the real options lens to examine CVC investments in cybersecurity startups, a combination of CVC and cybersecurity investments.

CVC investments in cybersecurity are typically motivated by two factors: technology positioning and future profit, both of which are compatible with the real options approach. Technology positioning investment in cybersecurity startups creates proprietary future access to technology (Benson and Ziedonis 2009; McGrath 1997), which would enhance the investing firm's competitive

advantage in terms of cybersecurity capability. On the other hand, profit-oriented organizational investments in startups are similar to venture capitalists' experimentation behavior, which generates exclusive rights for future pursuits (Kerr et al. 2014). In short, investments in cybersecurity startups create real options enabling technological and financial flexibilities (Tong and Li 2011; Trigeorgis 1993).

To apply the real options reasoning, a technology investment needs to satisfy three prerequisites: uncertainty in net payoffs, irreversibility in project costs, and managerial flexibility regarding the structure of the project (Dixit and Pindyck 1994). For the first condition, failure in entrepreneurship is known to be pervasive (Dimov and De Clercq 2006; Haswell and Holmes 1989; McGrath 1999), especially for the cybersecurity industry (Baker 2018). These failures can be caused by several reasons. For instance, cybersecurity innovation by the startup may fail to match the evolving techniques behind cyber-attacks (Baker 2018).

In addition, the investing firm's environmental uncertainty may also induce uncertainty in net payoffs (Havakhor and Sabherwal 2018). Moreover, investment in cybersecurity is traditionally viewed as a necessary cost-of-doing-business (Kvochko and Pant 2015), which adds to the uncertainty regarding net payoffs when mixed with profit motives of CVC investments. Regarding the second condition, organizational investments in startups are at least irreversible in the short run. While an investor may choose to sell its stakes in a startup, it could be challenging to find a buyer before the startup go public. Corporate investment in startups may also be irreversible in the long run if the investing company entered into a joint venture agreement with another party, which would be difficult to dissolve due to contractual obligations.

Finally, managers have ample flexibility in approaching cybersecurity startup investments. The manager has the flexibility to decide which startup to invest in, how much to invest, and whether to keep investing in the future. Apart from process flexibility, the manager is also flexible in interpreting the purpose of the investment. Investment in cybersecurity startups may be for financial speculations,

strengthening the investing firm's cybersecurity capability, or both. Hence, all three conditions for the real options reasoning hold for organizational investments in cybersecurity startups.

As a form of real options, CVC investments in cybersecurity will be met with economic rent for several reasons. Firstly, the real options is valuable in providing a window of opportunity for the latest cybersecurity technologies (Benson and Ziedonis 2009; Chemmanur et al. 2014; Park and Steensma 2012). With proprietary access to such technology, corporate investors can potentially mitigate future cyber-attacks, and capitalize on cybersecurity-related patents. An increase in digitalization (e.g. IoT) and hacking capabilities will make cutting-edge cybersecurity technologies even more indispensable. Consequently, the real options value of relevant cybersecurity technologies and expertise will continue to grow.

Secondly, while many cybersecurity startups go bankrupt within a few years (Baker 2018), uncertainty in the cybersecurity industry can potentially increase the value of CVC investments. Uncertainty is known to increase the real options value (Bloom and Van Reenen 2002; Tong and Li 2011), since securing complementary resources is more critical under uncertainties (Park and Steensma 2012). In addition, since acquiring IT startups in early stages is recommended under uncertainties (Ransbotham and Mitra 2010), CVC provides the option to defer potential acquisitions. Thus, CVC as a real option is particularly valuable in the uncertain cybersecurity industry.

Thirdly, with more media exposure of cybersecurity incidents, investors have conceivably become more aware of the consequences of data breaches and react positively towards counter-breach initiatives (e.g. cybersecurity CVC). Faced with potential economic consequences of data breaches (Campbell et al. 2003; Cavusoglu et al. 2004), investors will likely react positively towards indirect security investment (CVC), as they do with direct cybersecurity investments (Chai et al. 2011). Despite possible numbing towards prevalent data breaches, counter-breach initiatives are found to be associated with higher firm performance (Havakhor et al. 2018). Hence, investors will likely consider cybersecurity as an important issue to incentivize it by providing increased equity.

Finally, assuming market efficiency in dealing with real options, market investors are capable of evaluating the risks and benefits of investing in real options as they do with financial options (Cohen et al. 1972). Combined with an overall positive option value of cybersecurity CVC, we posit a positive association between cybersecurity CVC and firm performance.

3.3. Method

3.3.1 Data and sample

The hypothesis was evaluated based on a dataset of corporate investments in cybersecurity startups. To avoid any potential bias due to the 2008 financial crisis, only investments occurred after December 2008 were examined. We first identified cybersecurity startups using the categories in Crunchbase. Selected startup categories include "cybersecurity", "network security", "cloud security", "fraud detection", "intrusion detection", "identity management", etc. Next, organizational investors were identified based on investor categories. Eliminated investors were mainly independent venture capital (IVC) firms and angel investors.

After linking corporate investors with cybersecurity startups, we manually checked whether each investor was a regular organization (non-IVC). To test the effect of CVC investments on firm performance, organizational investors were confined to public firms or subsidiaries of public companies. Data from Crunchbase were merged with market data from CRSP and accounting data from Compustat by a fuzzy match of organization names. The name matches were then manually checked based on publicly available information. The final dataset consists of 873 firm-year observations, with 105 organizations that invested in 225 cybersecurity startups from 2009 to 2017.

3.3.2 Measures

The business value of investments in cybersecurity startups was assessed by the impact on a firm's Tobin's q, a ratio of market value versus book value. Tobin's q is considered appropriate in evaluating IT-related investments (Chari et al. 2008) since it is market-oriented and less sensitive to accounting practices (Bharadwaj et al. 1999). In our case, investments in cybersecurity startups create

real options that offer future access to proprietary technology as well as talent pools from the startup companies. Hence, the impact is best captured by Tobin's q, a forward-looking measure. A greater than 1.0 Tobin's q value indicates a positive investors' outlook for the real options values. Following (Bharadwaj et al. 1999), Tobin's q ratio is defined as

$$q = \frac{market\ value\ of\ equity + liquidating\ value\ of\ preferred\ stock + debt}{total\ assets}.$$

To assess a firm's investments in cybersecurity startups, we utilize two measures: a) a 0/1 dummy variable that is set at 1 if the firm makes an investment in one or more cybersecurity startups in a particular year (**Sec. Inv.**); b) the number of cybersecurity startups the firm invests in (**Sec. Inv. Num.**) in a year. While Crunchbase provides the amount of funding startups receive in each funding round, there is no information on the exact funding amount from each investor, as most funding rounds typically involve multiple investors. Hence, we resort to the dummy variable and investment counts.

We control for several industry- and firm-level variables. For industry-level controls, we define industries at the two-digit SIC code level. *Industry concentration* is estimated according to Herfindahl index as the market share of the top four companies in the industry. *Industry* q is calculated as the weighted average by total assets of each firm's Tobin's q in the industry. *Industry capital intensity* is also weighted by total assets. On the firm-level, typical financial variables are controlled. *Capital intensity* is the ratio between capital expenditure and total assets. *Market share* is the firm's percentage of sales in the two-digit SIC coded industry. *Firm size* is calculated as the natural log of the number of employees in the firm. *R&D* and *advertising* expenditure are estimated using the investment amount divided by the firm's annual revenue. Table 3.1 presents the mean and standard deviation of these variables, as well as correlations among them.

Table 3.1. Correlation Table

		Mean	SD	1	2	3	4	5	6	7	8	9	10
1	Tobin's q	1.551	1.748	1									
2	Ind. Con.	0.214	0.182	0.262	1								
3	Industry q	1.132	0.852	0.403	0.418	1							
4	Ind. Cap. Int.	0.027	0.022	0.117	0.152	0.410	1						
5	Cap. Intensity	0.030	0.037	0.184	0.025	0.123	0.381	1					
6	Market Share	0.029	0.049	-0.013	0.463	0.044	-0.037	-0.061	1				
7	Size	2.916	2.073	-0.233	-0.124	-0.229	0.099	0.116	0.394	1			
8	R&D	0.050	0.079	0.283	-0.060	0.299	0.260	0.024	-0.168	-0.316	1		
9	ADV	0.012	0.034	0.147	0.291	0.147	0.091	0.202	-0.024	-0.119	0.018	1	
10	Sec. Inv.	0.184	0.387	0.044	0.062	0.058	0.023	-0.027	0.154	0.093	0.004	0.046	1

$N = 873$. Ind. Con. = Industry concentration; Ind. Cap. Int. = Industry capital intensity; Sec. Inv. = Investment in cybersecurity startup

3.4 Analysis

To assess the effect of cybersecurity-related CVC investments on firm performance, the following equation is estimated.

$$q_{it} = \beta_1 \cdot sec\_inv_{it} + \beta_2 \cdot ind\_con_{it} + \beta_3 \cdot ind\_q_{it} + \beta_4 \cdot ind\_cap\_int_{it} + \beta_5 \cdot cap\_int_{it} + \beta_6 \cdot market\_share_{it} + \beta_7 \cdot size_{it} + \beta_8 \cdot R\&D_{it} + \beta_9 \cdot advertising_{it} + YEAR + INDUSTRY + \epsilon_{it}, \quad (3.1)$$

where subscripts i, t denote firm i in year t, and ϵ_{it} is the error term. We also test an alternative model with the security investment dummy (Sec. Inv.) replaced by the number of cybersecurity startups a firm invests in (Sec. Inv. Num.). In addition to year fixed effects, we include industry fixed effects instead of firm fixed effects due to the relatively small sample size. Firm-wise standard errors are clustered in the regression estimation.

Table 3.2 presents the main regression results. Based on the fixed-effect model (equation 1), we observe a significant positive effect of cybersecurity CVC investments towards the investing firms' Tobin's q. The positive effect hold for both the dummy variable (Sec. Inv.) and the number of investments (Sec. Inv. Num.). Notably, the effect size is larger and more significant for the main model using the cybersecurity CVC dummy, suggesting that investors may be more sensitive to the fact that organizations engage in cybersecurity CVC(s) than the extent of the engagement. Overall, the results suggest the market recognizes the positive real options value for cybersecurity CVCs.

Table 3.2. Main Results

DV=Tobin's *q*	Coefficient	S.E.	Coefficient	S.E.
Sec. Inv.	**0.246****	**0.116**		
Sec. Inv. Num.			**0.104***	**0.056**
Ind. Con.	2.852**	1.181	2.853**	1.179
Industry *q*	-0.147	0.193	-0.145	0.193
Ind. Cap. Int.	-6.324	4.408	-6.377	4.423
Cap Intensity	8.259**	3.214	8.262**	3.236
Market Share	0.378	2.535	0.331	2.549
Size	-0.063	0.076	-0.063	0.076
R&D	4.834***	1.734	4.844***	1.748
ADV	0.051	3.670	0.145	3.672
Constant	1.047**	0.466	1.054**	0.465
Fixed Effects	Industry & Year		Industry & Year	
Observations	873		873	
R-squared	0.364		0.363	

$*\ p < 0.10$; $**\ p < 0.05$; $***\ p < 0.01$. Ind. Con. = Industry concentration; Ind. Cap. Int. = Industry capital intensity; Sec. Inv. = Investment in cybersecurity startups; Sec. Inv. Num. = number of investment in cybersecurity startups

Table 3.3. Robustness Checks

	(1) Current Year ROA	(2) Next Year ROA	(3) Current Year ROS	(4) Next Year ROS
Sec. Inv.	**0.019***	**0.021***	**0.747***	**0.834**
	(0.011)	**(0.012)**	**(0.442)**	**(0.583)**
Industry Con.	0.136*	0.161**	-1.931	2.172
	(0.070)	(0.072)	(1.499)	(1.711)
Industry *q*	0.009	0.009	-0.203	-0.534
	(0.026)	(0.015)	(0.391)	(0.585)
Ind. Cap. Int.	0.198	0.226	16.449	8.227
	(0.397)	(0.326)	(13.063)	(10.165)
Cap Intensity	0.008	0.138	-10.368	-0.550
	(0.247)	(0.171)	(8.132)	(2.355)
Market Share	-0.377	-0.471**	1.176	-13.933
	(0.237)	(0.228)	(5.701)	(9.766)
Size	0.025**	0.028***	-0.034	0.697
	(0.010)	(0.010)	(0.205)	(0.482)
R&D	-1.293**	-0.425*	-66.657**	-10.079
	(0.508)	(0.249)	(27.989)	(10.263)
ADV	-0.015	0.146	0.386	6.148
	(0.325)	(0.221)	(14.412)	(5.222)
Constant	-0.058	-0.049	3.411	-1.285
	(0.066)	(0.037)	(2.072)	(1.163)
Fixed Effects	Industry & Year	Industry & Year	Industry & Year	Industry & Year
Observations	875	758	874	757
R-squared	0.462	0.344	0.577	0.217

$*\ p < 0.10$; $**\ p < 0.05$; $***\ p < 0.01$. Ind. Con. = Industry concentration; Ind. Cap. Int. = Industry capital intensity; Sec. Inv. = Investment in cybersecurity startups.

While Table 3.2 points to the positive effect of cybersecurity CVCs towards Tobin's q, it is not clear whether the market-oriented valuation is realized in firms' bottom-line values assessed by traditional accounting measures. Robustness was tested by replacing the dependent variable Tobin's q with return on assets (ROA) and return on sales (ROS). The results are reported in table 3. In both ROA and ROS models, the effect size of cybersecurity CVCs increases from year t to $t + 1$, demonstrating the lag effects of the traditional accounting measures. Taken together, the profitability impact of cybersecurity CVC becomes more visible over time.

Since the main motive for CVC investments is to gain a window of opportunities on the latest technologies (Benson and Ziedonis 2009), and cybersecurity technologies may carry different weights for different types of firms, the effect of CVC on firm performance may differ based on the nature of the business. For instance, IT firms may possess higher absorptive capabilities for cybersecurity technologies than non-IT firms, hence they will likely benefit more from CVC investments in cybersecurity (Dushnitsky and Lenox 2005a; Dushnitsky and Lenox 2005b). Additionally, IT firms are more likely to have related R&D investments, which are known to complement CVC investments (Benson and Ziedonis 2009). As such, the main model was tested on subsamples of IT and non-IT firms. The firms were categorized based on two-digit SIC codes. As expected, the effect of cybersecurity CVC is larger and more significant for IT firms (Table 3.4).

Apart from firm types, we also take into consideration the macro cybersecurity environment. Since cybersecurity incidents have been on the rise in the past decade (Accenture 2017), we expect a more pronounced effect in recent years. The firm-year sample was split into two parts based on the year. From January 2009 to June 2013, cyber risk is considered relatively low. From July 2013 to December 2017, cyber risk is considered relatively high. Under higher cyber-risks, cybersecurity technology would be valued higher. Thus, more recent investments in cybersecurity startups will generate more business value. Indeed, the subsample analysis suggests the effect is stronger and more significant in recent years (Table 3.4).

Table 3.4. Subsample Analyses

DV = Tobin's q	(1) IT Firms	(2) Non-IT Firms	(3) High Cyber Risk	(4) Low Cyber Risk
Sec. Inv.	**0.368***	**0.061**	**0.335****	**0.074**
	(0.185)	**(0.105)**	**(0.142)**	**(0.208)**
Industry Con.	2.653*	2.700*	3.664**	2.345**
	(1.572)	(1.407)	(1.583)	(1.017)
Industry q	0.351	-0.293	-0.263	-0.560
	(0.288)	(0.214)	(0.319)	(0.546)
Ind. Cap. Int.	-13.418	-11.326	-6.051	-1.487
	(8.033)	(12.025)	(5.358)	(5.827)
Cap Intensity	6.782	10.172***	1.947	14.981***
	(4.532)	(3.404)	(2.253)	(5.145)
Market Share	1.291	1.987	-0.659	0.144
	(4.782)	(2.992)	(2.867)	(2.164)
Size	-0.309*	-0.006	0.014	-0.103
	(0.156)	(0.085)	(0.071)	(0.081)
R&D	6.079**	4.115**	5.056**	6.245***
	(2.764)	(1.849)	(1.972)	(1.848)
ADV	2.674	1.483	0.644	-0.256
	(5.732)	(3.618)	(4.758)	(3.696)
Constant	1.223**	1.121*	0.756*	1.258*
	(0.605)	(0.623)	(0.435)	(0.651)
Fixed Effects	Industry & Year	Industry & Year	Industry & Year	Industry & Year
Observations	320	553	472	401
R-squared	0.403	0.385	0.428	0.395

$* p < 0.10$; $** p < 0.05$; $*** p < 0.01$. Ind. Con. = Industry concentration; Ind. Cap. Int. = Industry capital intensity; Sec. Inv. = Investment in cybersecurity startups.

3.5 Discussion

Overall, the findings of this study suggest that CVC investments in cybersecurity are met with positive economic rewards, although the intensity of such rewards may depend on the business nature of the investing firm and the macro cybersecurity risk-level. In addition, our findings suggest that accounting measures of profitability (ROA, ROS) are also positively associated with corporate investments in cybersecurity startups.

Before discussing the implications of the findings, we acknowledge some limitations of this study. First, only public firms are included in the sample to ensure the availability of firm performance data. Some sizable private corporations may also engage in CVC in cybersecurity. While private companies may be less susceptible to reputation damage associated with data breaches, they are still subject to financial losses as well as government fines, hence will likely benefit from

cybersecurity CVCs as well. Second, we did not incorporate environmental uncertainties for the investing firms in our model. Further studies can tease apart the environmental factors (environmental dynamism, complexity, munificence) for the investing firms (Xue et al. 2012). As we focused on one industry (cybersecurity) for startups, environmental uncertainty for startups was assumed to be consistent in each year. Third, since the knowledge creation rate and the number of CVC investments have a curvilinear relationship (Wadhwa and Kotha 2006), the relationship between the number of CVC investments and firm performance will likely follow a similar pattern. Initially, with only a few investments, investors may react strongly towards a high knowledge creation rate as a result of CVC investments. As investments grow in number, the marginal benefit may decrease. Our linear treatment did not take into account such intricacies, which may be a possible reason for a less significant result in the second model in table 2.

Despite these limitations, this paper has a few theoretical implications. The study contributes to the literature on three fronts. First, this paper adds to the economics of cybersecurity literature by demonstrating the overall positive value of organizational investments in cybersecurity startups, despite the cost nature of general cybersecurity investments. Second, parallel to the profitability of direct cybersecurity investments (Chai et al. 2011), this study demonstrates the positive value of indirect cybersecurity investments through investments in relevant startups. Although investments in startups can be risky, it provides a window for cutting edge technologies and expertise that are less accessible by direct cybersecurity investments. We have shown that these forward-looking investments, conceptualized as real options, also enhance firm value. Third, the paper adds to the CVC literature by revealing the tangible value of organizational investments in non-rent-seeking technologies. While CVC literature has utilized the real options lens in evaluating investment choices (Tong and Li 2011) and general technology acquisitions (Ceccagnoli et al. 2017), the study suggests that a seemingly less profit-oriented technology can also generate positive real option values, and consequently increases firm value.

For managers, this paper has revealed the profitability of a new avenue for cybersecurity investments. With ever-increasing hacking threats, companies need to possess the most up-to-date cybersecurity technologies. While direct investments in current cybersecurity technologies are essential, cybersecurity technologies may become outdated more quickly than other types of technologies such as enterprise resource planning systems. Apart from passively matching the current technology, companies can acquire options for future cybersecurity technologies and talent pools through indirect cybersecurity investments in startups. As a forward-looking cybersecurity measure and investment strategy, CVC investments in cybersecurity also add tangible value to the firm.

CHAPTER IV: CYBERSECURITY LEGISLATION AND DIGITIZATION[18]

4.1 Introduction

Digitization, i.e., using information technologies (IT) and computational services to automate, streamline, and intelligize work processes and their end products, has been the cornerstone of economic growth and prosperity in the past two decades. At the same time, the uptake in digitization has coincided with the rise of cybersecurity breaches that target digital records and traces, and in many cases, threaten the economic viability of growing and established corporations alike. As such, identifying cybersecurity breaches and handling them effectively has become a key area of investment with a cost nature to shield corporations from the unintended consequences of digitization. Therefore, organizations undergoing digitization efforts are continually faced with a difficult question: do the costs of dealing with the rising cybersecurity threats turn digitization efforts to less attractive options? For the policymakers concerning digital development, the question morphs into whether or not the costs of dealing with cybersecurity threats set entry barriers for digitizing entities and stifle digital growth.

A straight-forward answer to the above questions is hard to obtain at a corporate level because identifying canceled or reduced-in-size plans of digitization, as well as understanding the internal cost-benefit calculus behind such plans, is cumbersome due to a lack of detailed public records. However, legal changes triggering an increase in cybersecurity expenditure provide an opportunity to find some answers to those questions. This study capitalizes on one such opportunity.

[18] We thank the participants of the 2019 ICIS, 2019 ICIS doctoral consortium, 2019 AMCIS doctoral consortium, Mohammad Saifur Rahman, Gurpreet Dhillon, and Shuyuan Mary Ho.

By the end of 2018, all states in the US have passed security breach notification laws (SBNLs), requiring organizations to notify consumers and other entities19 regarding breach of personal identifiable information. While SBNLs reduce risks for consumers (Kwon and Johnson 2014; Romanosky et al. 2011) and shareholders (Ashraf and Sunder 2018), the imposed compliance costs on organizations could incur barriers for digitization initiatives. These barriers may be magnified by the increased cyber-threats (Sen 2018) and the shortage of cybersecurity talents (Zadelhoff 2017). It is therefore important to understand the broader questions discussed above by studying how SBNLs affect digitization. Since the main procurers of digitization are IT service firms and employment is a fundamental indicator of economic dynamism (Bravo-Biosca et al. 2016), we focus on the influence of SBNLs on the increase or decrease in employment by IT service industries.

SBNLs will impact IT service firms in several ways. On one hand, mandatory reporting requirements further expose organizations to financial and reputational loss associated with data breaches. Firms with existing digital infrastructure will be incentivized to increase cybersecurity budgets, thus creating jobs for cybersecurity firms, a subset of IT service providers. Enhanced security will also boost consumer trust in digital goods and services, thereby benefiting general IT service providers. On the other hand, cybersecurity requirements could create barriers for digitization. Organizations will be discouraged from engaging in new digitization initiatives or expanding existing ones and thereby destructing jobs for general IT service providers. In addition, the severe shortage of cybersecurity labor (Zadelhoff 2017) will limit organizations from engaging in digitization initiatives even when they are economically viable. The increased entry barrier to digitization will therefore negatively influence the employment of IT service providers. With competing influences, this study empirically examines how the enactment of SBNLs affects the employment of IT service providers (RQ).

We exploit the staggered passages of state-level SBNLs, i.e., passages that happen at different points of time, to identify their effect on the employment of IT service providers. Using a difference-

[19] Other notification entities typically include state attorney generals, consumer report agencies, third-parties that own the data.

in-difference design, we found that enactments of SBNL reduce employment for larger and more mature IT service firms, but have no effect towards smaller and younger firms. The main results are obtained after controlling for various state-level economic variables (unemployment rate, personal income growth rate, housing price index). Since our analysis suggests state economic and political conditions do not predict the passage of the laws, SBNLs enactments can be viewed as an approximate random assignment. Several robustness checks were conducted by including controls such as local sentiments about data breaches and the number of compromised records, and excluding observations around the 2008 financial crisis, as well as observations from California and Massachusetts, where IT industries are more vibrant. To further alleviate identification concerns, we tested the main model using a placebo timing and a placebo industry.

This paper appeals to three groups of audiences. First, the study will add to the economics of digitization literature, which has traditionally focused on cost reduction through digitization (Goldfarb and Tucker 2019). While cybersecurity adds cost to digitization, the issue lies in measuring its impact on the digital economy. The staggered passage of SBNLs provides a unique opportunity to identify the impact of cybersecurity on digitization. We show that the raised cybersecurity standards may become entry barriers for digitization, as reflected by the employment reduction of larger and more mature IT service providers. While prior literature has revealed the social costs of digitization (Chan and Ghose 2013; Chan et al. 2019), this study documents an economic cost of digitization.

Second, this paper adds to the cybersecurity literature by revealing the economic implications of legislative mitigation strategies. Prior cybersecurity literature has shown that cybersecurity legislation reduces security threats (Hui et al. 2017; Kwon and Johnson 2014; Romanosky et al. 2011), whereas the broader and unintended economic impact of such legislation is understudied. With cyber threats becoming more severe (Sen 2018), an emerging stream of literature focuses on whether cybersecurity investments can effectively prevent data breaches in key industries, such as the healthcare industry (Angst et al. 2017; Kwon and Johnson 2013; Kwon and Johnson 2014; Kwon and Johnson 2018).

This paper takes a different focus and quantifies the economic impact of variation in the regulatory environment of cybersecurity investments.

Third, this paper will shed light on legislative discussions regarding cybersecurity. Similar discussions exist around privacy laws. For example, previous research unfolded that the compliance cost associated with healthcare privacy laws discourages electronic medical record adoption in hospitals (Miller and Tucker 2009). We focus on a different set of state-level legislation and explore beyond the healthcare industry. While politicians face increasing consumer pressure in holding organizations accountable for data breaches, it is also important to understand the costs and benefits of these laws to the critical areas of the economy such as employment. With all states now having passed SBNLs, this paper will add to the discussions of a federal-level SBNL.

The rest of the paper will proceed as follows. We will first provide some background of SBNLs, and show that state-level economic, political, and legal environments do not predict passages of SBNLs. We will then explain the data sources used in the study, IT service industries classifications, firm-age and size classifications, and measurement of various constructs. Specifications of the generalized difference-in-difference (DID) design will be discussed. The main analyses will be followed by various robustness and placebo tests. We will conclude with discussions of limitations and implications of the study.

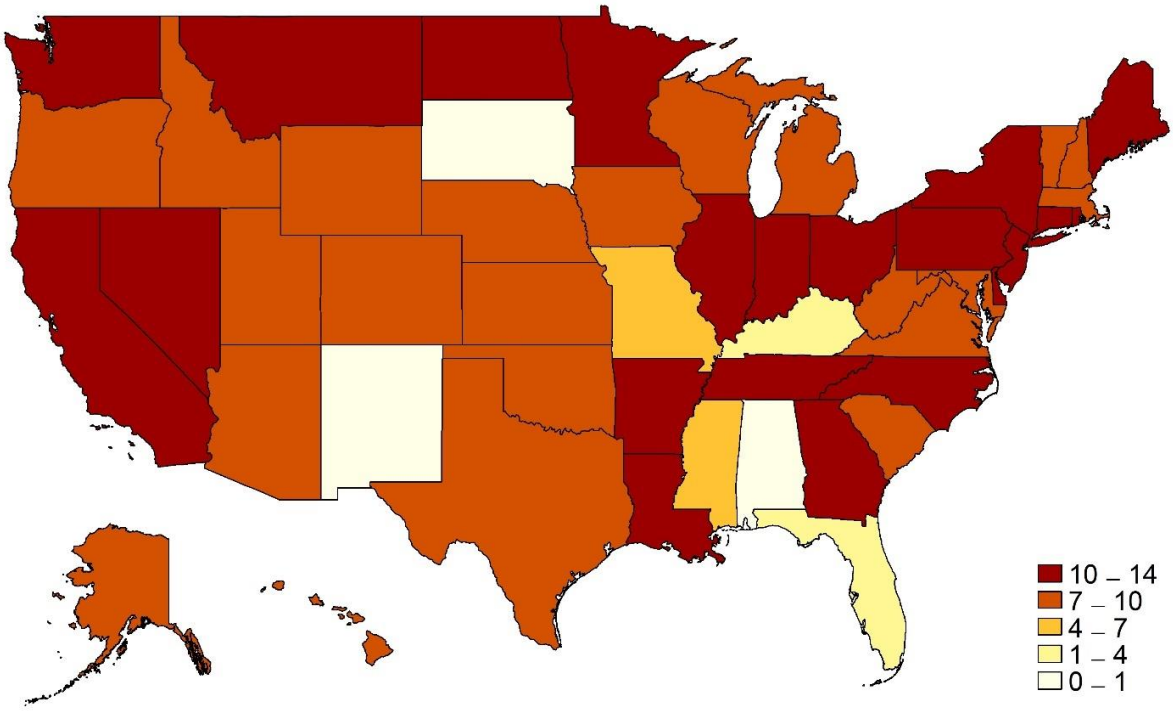
4.2 Institutional background

The state-level security breach notification law (SBNL) was first introduced in California in 2002. By the end of 2018, all states have passed some version of the law. Figure 4.1 depicts the number of years since the enactment till the end of 2016. All SBNLs require organizations to notify customers in a timely manner when their personal identifiable information is breached through the organizations. Many states impose hard deadline such as 30 or 45 days to notify the affected party after a breach is discovered. Notification channels include written notice, email, phone call, etc. Some states allow exemptions if after investigation the company can provide written proof that the security

breach will not harm the consumers. Apart from notifying customers, SBNLs often include notifications to state attorney generals, consumer report agencies and third-parties that own the data.

Most of these notifications are only necessary if the number of compromised records exceeds a certain threshold. Personal identifiable information (PII) in SBNLs include name, social security number, driver's license number, state ID number, account number, credit/debit card number, pin, passwords. Some states define PII more broadly to include medical information and biometric information (e.g. fingerprint). A few states allow private citizens to pursue civil litigations against the entities that fail to comply with SBNLs. A federal-level SBNL was proposed in 2015 (Shear and Singer 2015), but did not pass the congress.

Figure 4.1 Years since Enactment of Security Breach Notification Law till the End of 2016



Needless to say, SBNLs were passed in order to mitigate cyber threats. More recent enactment of SBNLs may be partly due to the high-profile breach cases, such as the incident with Equifax in 2017. Because if penalties are associated with failure to comply, the passage of SBNLs puts a coercive institutional pressure on firms to update their cybersecurity practices or initiate new projects

that enable compliance. Although the passage of SBNLs creates a suitable quasi-experimental setting to study the impact of cybersecurity initiatives on the digital growth, a key question is whether or not the passages of those laws resemble a random assignment of treatment. Acknowledging that a full random assignment is far from the realities of policymaking, our first step in the study was to ensure that the known factors influencing state policy did not systematically influence the enactments of SBNL.

Table 4.1 provides an exogeneity check for the SBNL passages. We investigate whether a state's macroeconomic, political economy, or legal conditions predict the passage of the SBNL, following Appel et al. (2019). The SBNL dummy is set to 1 if the law is passed in the state, and o otherwise. The Democratic and Republican control (Dem/Rep_State) dummies indicate a party controls both the legislative and executive branches. The dummies equal 1 if both branches are controlled by the democratic/republican party, respectively, and equal to 0 for split controls. The legal ranking measures the business friendliness of the state legal system through the lawsuit climate survey conducted by the US Chamber of Commerce. The local sentiment of data breaches (GSV_Data_Breach) is measured by the Google search volume of the keyword "data breach". To avoid over-fitting, we did not include the state fixed effects in the logistic regression. The non-significant coefficients in Table 4.1 suggest that persistent state characteristics that may correlate with the passage of SBNLs do not undermine the validity of our difference-in-difference design.

Linear regressions with inclusion and exclusion of predictors following Appel et al. (2019) produce similar results (Appendix D). We choose to report the logistic regression in Table 4.1, since linear probability models can potentially give rise to estimated probabilities that exceed 1 or fall below 0. While treatments in quasi-experiments are not randomized by and large (Angrist and Pischke 2009), the predictive regression suggests the assignment of SBNLs is a close approximation to randomization.

Table 4.1. Predictive Regression

	SBNL
Unemployment_Rate	0.053
	(0.29)
Personal_Income_Growth	-14.391
	(13.33)
Housing_Price_Index	0.005
	(0.94)
Dem_State	0.293
	(0.58)
Rep_State	-0.687
	(1.57)
Legal_Rank	-0.016
	(1.07)
GSV_Data_Breach	-0.769
	(1.09)
Year-quarter FE	Yes
Observations	323

Notes. Robust standard errors are in parentheses. The sample size is small compared to the main analyses in Table 3, because in some quarters, no state passed the law, and year-quarter fixed effects perfectly predict the SBNL dummy. These observations are dropped in the logistic regression. State-year-quarter observations after the law passages are dropped, following Appel et al. (2019).

4.3 Method

4.3.1 Data and Sample

State-level employment data is obtained from the Census Bureau's Quarterly Workforce Indicators (QWI). For each state-quarter, the QWI reports employment data aggregated by firm age, size and four-digit North American Industry Classification System (NAICS). The QWI dataset divides firm age into five groups: 0-1, 2-3, 4-5, 6-10, 11+. In measuring the impact on employment, we collapse the firm age categories to three: 0-3, 4-10, 11+ years following Appel et al. (2019), where firms aged 0-3 are considered startups. The QWI dataset divides firm sizes based on the number of employees: 0-19, 20-49, 50-249, 250-499, 500+. For symmetry with firm age categorization, we collapsed firm sizes into three categories: 0-49, 50-499, 500+.

To identify IT service industries, we follow the classification by the Census Bureau using the four-digit NAICS code (Haltiwanger et al. 2014) (see Table 4.2). Signed and effective dates of SBNLs are collected from the National Conference of State Legislatures (NCSL) and Perkins Coie.

The sample period is from 2001 to 2016, one year before the first state SBNL enactment, and up to the latest QWI data availability. The main analysis with firm-age categorization has 3358 state-year-quarter observations. The sample size varies for subsequent analyses based on data availability. Computers and communication industries are used as a placebo in additional identification analyses.

Table 4.2. Industry classification

NAICS (2017)	Industry Description
IT Services	
5112	Software publishers
5191	Internet publishing and broadcasting
5182	Data processing, hosting, and related services
5415	Computer systems design and related services
Computers & Communications	
3341	Computer and peripheral equipment manufacturing
3342	Communications equipment manufacturing
3344	Semiconductor and other electronic component manufacturing
3345	Navigational, measuring, electromedical, and control instruments manufacturing
5179	Other telecommunications

Notes. The NAICS classification do not specify cybersecurity service providers. Internet services industries were treated as IT service providers. Computers & communications industries were used as a placebo industry in table 6.

4.3.2 Measures

The dependent variable, **employment** in IT service firms is measured as the natural logarithm of one plus the number of full quarter employment (emps in QWI), i.e., the number of jobs that are held on both the first and last day of the quarter with the same employer. Notably, employment by IT service providers includes but is not limited to IT labor. However, since QWI data are aggregated on the plant level, for a large and diversified company with multiple subsidiaries, most of its non-IT employment is not included in our data if the IT subsidiary has a different physical location. Nevertheless, even within an IT subsidiary, there are some non-IT employees in the back office, which cannot be purged out due to data limitations. At any rate, non-IT employment change in IT service industries shall also reflect the change in the supply of digital goods and services. When an IT service provider has more business opportunities, it will hire more IT as well as non-IT staffs.

Our main explanatory variable, $\boldsymbol{SBNL_{st}}$, is an indicator set to one if SBNL has been signed into law in state s on or before year-quarter t, and zero otherwise. In a *pilot* study, we codified SBNLs based on the five dimensions in Ashraf and Sunder (2018): a) whether a notification law imposes a

hard deadline following the discovery of a data breach; b) if a law requires firms to disclose a data breach only if it is determined to reasonably likely to cause harm to the victims; c) if a law requires notification to the attorney general or other state agencies; d) if a law allows private citizens to pursue litigation against a firm that fails to comply with the data breach disclosure law; and e) if a law defines personally identifiable information more broadly than general. While the codification is a more detailed depiction of the law, we found no significant effect towards IT employment in the main and robustness analyses, suggesting that passage of SBNL play a more dominant role than details of the law. The codification is hence omitted in subsequent analyses.

For control variables, we obtained state-level quarterly u*nemployment rate*, *personal income growth rate* from the Bureau of Economic Analysis (BEA). The *housing price index*, obtained from the Federal Housing Finance Agency, is measured by the average price changes in repeated sales or refinancing on the same properties. While the underlying assumption of natural experiments is that control and treatment groups have similar characteristics except for the treatment, it would be naïve to assume different states possess identical economic backgrounds (e.g. Wyoming and New York). Hence, the three variables serve as controls for state-level economic conditions.

4.3.3 Specification

In an ideal experimental setting at the firm level, identical SBNL treatments would be randomly assigned to each individual firm, and employment at the firm level can be measured at different points in time, so that we can precisely identify how SBNLs affect different types of IT service providers over time. In lieu of the ideal setting, analyses are conducted on a state-year-quarter level following a quasi-experimental design, where enactments of SBNL (treatment) approximates random assignment (Table 4.1).

We employ a generalized difference-in-differences (DID) specification at the state-year-quarter level following Bertrand and Mullainathan (2003). In this case, an event study would not accurately capture the effect of SBNLs due to the lack of control and treatment groups, whereas a simple DID specification would not be compatible with the staggered nature of legislation enactments. Recent

studies that involve staggered exogenous shocks have used similar specifications (Appel et al. 2019; Ashraf and Sunder 2018; Chan et al. 2019). Our main analysis uses the following equation.

$$Employment_{st} = \alpha_s + \alpha_t + \delta \cdot SBNL_{st} + \gamma X_{st} + \epsilon_{st},$$

where α_s is a state fixed effect, which controls for state characteristics that do not vary over the sample period. α_t is a year-quarter fixed effect, which absorbs aggregate shocks affecting all states. X_{st} are control variables (state-level unemployment rate, personal income growth rate, housing price index). ϵ_{st} is an error term. Finally, the coefficient δ is the DID estimator for the effect of SBNL enactments towards the employment of IT service firms.

This specification allows the same states to be part of the treatment and control groups at different points in time. The treatment group consists of states passing a law at year-quarter t, i.e., the states experiencing the exogenous shock. The control group includes all states not passing a law at year-quarter t, regardless of whether they have or will pass a law (Angrist and Pischke 2009; Bertrand and Mullainathan 2003). This means the SBNL dummy may be equal to 1 and the state can still be in the control group. In essence, the generalized DID design enables the construction of a control group even when all states have (eventually) passed the law, as long as the passages are staggered.

4.4 Results

The main results (Table 4.3) show that the employment of IT service industries decreases following the passages of SBNL relative to states not passing the law, suggesting an adverse effect of SBNLs towards digitization. Column 1 and 5 show an overall decline across firm age and size categories. The two columns produce different coefficients because QWI, for privacy reasons, reports missing data for industries with low employment number, and aggregating employment data from different industries make it appear as if there is no data missing. Columns 2, 3, and 6 produce insignificant coefficients, suggesting that SBNLs have no obvious impact on the employment by newer and smaller firms. The negative effect is significant for firms aged eleven years or older (column 4), and for medium and large firms with at least 50 employees (column 7 and 8). Subsequent

tests reveal the result on mid-size firms (column 7) is not robust (robustness tests on column 7 are not reported for brevity). Hence, the overall decline is mainly driven by mature (11+ years) and large (500+ employees) firms.

This concentrated results on large and mature firms are likely because younger IT service firms are more agile relative to mature ones, and hence are more likely to swiftly cater to the portion of customer firms that keep their digitization projects with higher cybersecurity standards. Therefore, the results may suggest that the supply of cybersecurity compliance services is concentrated in small and new firms, hence shielding them from the overall adverse impacts of a decrease in non-cybersecurity service demand.

Table 4.3. Main results

	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
		Firm Age (Years since founding)				Firm Size (# of Employees)		
	All ages	0-3	4-10	11+	All sizes	0-49	50-499	500+
SBNL	-0.058**	-0.061	-0.033	-0.056**	-0.069*	-0.035	-0.098**	-0.119**
	(0.029)	(0.071)	(0.053)	(0.026)	(0.035)	(0.030)	(0.038)	(0.054)
Unemployment	-0.018*	-0.011	-0.001	-0.020*	-0.019*	-0.014*	-0.030	-0.023
	(0.009)	(0.017)	(0.015)	(0.011)	(0.009)	(0.007)	(0.019)	(0.019)
PI Growth Rate	0.366	0.244	0.418	0.455	0.290	0.106	0.056	-0.261
	(0.238)	(0.742)	(0.359)	(0.327)	(0.243)	(0.165)	(0.396)	(0.650)
Housing_Price	0.000	0.000	0.001	-0.000	0.000	0.001**	0.000	0.000
	(0.000)	(0.001)	(0.001)	(0.000)	(0.000)	(0.000)	(0.001)	(0.001)
State Fixed Effects	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Year-Quarter Fixed Effects	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Observations	3,358	3,358	3,358	3,358	3,358	3,358	3,358	3,358
R-squared	0.995	0.971	0.980	0.992	0.994	0.996	0.981	0.906

*Notes. Robust standard errors clustered by the state are reported in parentheses. ***, **, and * denote significance at the 1%, 5%, and 10% level, respectively. PI growth rate stands for personal income growth rate.*

With results mainly driven by mature (age 11+) and large firms (500+ employees), the robustness checks in Table 4.4 focus on these firms exclusively. We found consistent results under various specifications and sample periods. In column 3, we controlled for the natural logarithm of one plus the number of compromised records (starting from 2005, from Privacy Rights Clearinghouse) in each state and year-quarter to ensure that the level of actual cyber threats, irrespective of legislative pressure, do not drive the findings. In column 4, we controlled for the local sentiment for breaches,

measured by the Google search volume (GSV) index for the search term "data breach" (starting from 2004). Since the 2008 financial crisis may have affected all 50 states unevenly, we excluded data from the last quarter in 2007 till the second quarter in 2009 (column 1), and test for post-crisis results (Column 2-4). As IT industries in California and Massachusetts are more vibrant, analyses excluding both states (Column 5) suggest the results are not driven by individual states. Column 6 reports weighted regressions with weights based on the natural logarithm of each state's employment in 2001, the first year in the sample. Finally, we tested all models using beginning of quarter and end of quarter employment (emp and empend in QWI, respectively). We also tested the models using the un-collapsed firm age and size categories in QWI. The alternative employment measures and analyses with un-collapsed categories produce similar results[20].

To inspect the timeline of the impact of SBNLs, we added additional dummies in the main regression model (Table 4.5), where $SBNL[iQ]_{st}$ is set to one if SBNL is effective i quarters before year-quarter t for state s, and zero otherwise. $SBNL[4Q_{+}]_{st}$ is set to one if SBNL is effective four quarters or more before year-quarter t for state s, and zero otherwise. We observe an increase in effect size following the event quarter, with the results concentrated on more mature and larger firms (see also Figure 4.2), similar to our main findings. The significant negative coefficients for $SBNL[4Q_{+}]_{st}$ and the large effect size suggests the negative impact would likely persist beyond the fourth quarter following the enactments of the law.

To further alleviate identification concerns, we tested the main model using a placebo timing and a placebo industry (Table 4.6). Placebo timing is set at twelve quarters before the event (column 1, 2) following Appel et al. (2019). The non-significant DID estimators mitigate concerns that confounding events coincide with the SBNLs' enactment timing were driving the main results. Placebo tests with the false timing for other age and size categories produced similar non-significant coefficients, and are omitted for brevity.

[20] The results using alternative employment measures and un-collapsed firm age and size categories are available upon request.

Table 4.4. Panel A. Robustness check I. (Firm age=11+)

VARIABLES	(1) Exclude-Crisis	(2) Post-Crisis	(3) Post-Crisis	(4) Post-Crisis	(5) No CA&MA	(6) Weighted Regression
SBNL	-0.062**	-0.095*	-0.095*	-0.095**	-0.051*	-0.080***
	(0.026)	(0.048)	(0.048)	(0.047)	(0.027)	(0.025)
Unemployment	-0.020	-0.022*	-0.022*	-0.022*	-0.020*	-0.021*
	(0.012)	(0.011)	(0.011)	(0.011)	(0.011)	(0.012)
Personal_Income_Growth	0.572*	0.331	0.336	0.330	0.392	0.657
	(0.318)	(0.476)	(0.470)	(0.478)	(0.323)	(0.450)
Housing_Price	-0.000	-0.000	-0.000	-0.000	-0.000	0.000
	(0.000)	(0.001)	(0.001)	(0.001)	(0.000)	(0.000)
Ln(Data_Breach)			0.001			
			(0.001)			
GSV_Data_Breach				0.001		
				(0.002)		
State Fixed Effects	Yes	Yes	Yes	Yes	Yes	Yes
Year-Quarter Fixed Effects	Yes	Yes	Yes	Yes	Yes	Yes
Observations	3,008	1,719	1,719	1,719	3,259	3,358
R-squared	0.992	0.997	0.997	0.997	0.991	0.990

Panel B. Robustness Check II (# of Employees=500+)

VARIABLES	(1) Exclude-Crisis	(2) Post-Crisis	(3) Post-Crisis	(4) Post-Crisis	(5) No CA&MA	(6) Weighted Regression
SBNL	-0.131**	-0.168***	-0.168***	-0.167***	-0.109*	-0.133**
	(0.054)	(0.062)	(0.062)	(0.062)	(0.056)	(0.058)
Unemployment	-0.021	-0.024	-0.024	-0.024	-0.021	-0.031*
	(0.020)	(0.016)	(0.016)	(0.016)	(0.019)	(0.018)
Personal_Income_Growth	-0.219	0.319	0.344	0.320	-0.319	0.535
	(0.705)	(0.617)	(0.598)	(0.615)	(0.647)	(0.737)
Housing_Price	0.000	-0.000	-0.000	-0.000	0.000	0.001
	(0.001)	(0.001)	(0.001)	(0.001)	(0.001)	(0.001)
Ln(Data_Breach)			0.003			
			(0.003)			
GSV_Data_Breach				-0.001		
				(0.003)		
State Fixed Effects	Yes	Yes	Yes	Yes	Yes	Yes
Year-Quarter Fixed Effects	Yes	Yes	Yes	Yes	Yes	Yes
Observations	3,017	1,720	1,720	1,720	3,267	2,444
R-squared	0.898	0.965	0.965	0.965	0.912	0.985

*Notes. Robust standard errors clustered by state are reported in parentheses. ***, **, and * denote significance at the 1%, 5%, and 10% level, respectively. Crisis is defined as the financial crisis from Q4 in 2007 to Q2 in 2009. CA and MA are short for California and Massachusetts. GSV_Data_Breach stands for the Google search volume index of "data breach" on the state level (starting from 2004).*

We chose the computers and communications industry as a placebo since it is most similar to the IT service industry (see Table 4.2), and the two industries will likely follow similar business cycles. Hence, the placebo test can potentially address concerns about omitted variables that correlate with

the IT business cycles and the passages of SBNL. Unlike IT service firms, however, manufacturers of personal computers and cellphones are unlikely to be affected by the law changes, as everyday consumers are certainly not personally subject to SBNL compliance. In addition, cloud-based computing has also reduced the demand for a hardware update in digitization. The industry classifications follow Haltiwanger et al. (2014). Since the computers and communications industries are predominantly in the manufacturing business, it is more labor-intensive and should be more sensitive to macro changes that would alter its employment. However, except for column 7 in Table 6, all DID estimators in columns 3-8 are non-significant, suggesting that SBNLs have no significant impact on employment in the placebo industry, thus alleviating concerns that macro conditions that reduce employment across different industries were driving the results.

Overall, the results show no significant effect using either the placebo timing or the placebo industry, which gives us more confidence to attribute the change in employment of IT service industries to SBNL enactments. Finally, while the parallel-trends assumption in DID is ultimately untestable, there is some indirect evidence. We found no significant difference in the evolution of employment in treated and controlled states prior to the passage of SBNL for all firms (confidence intervals in Figure 4.2 and Appendix E before the event intersect with the horizontal zero lines).

Figure 4.2 Evolution of Employment by IT Service Providers
The figures below plot the evolution of IT employment at mature IT firms (left graph) and large IT firms (right graph) in treatment groups relative to the control groups. The y-axis represents the coefficients on the dummy variables indicating the timing of breach notification law passage and the x-axis represents the event quarter centered around the quarter when breach notification law is signed (Event Quarter=0). The dots represent the point estimates and the vertical bars represent the 95% confidence intervals (see also table 4.5).

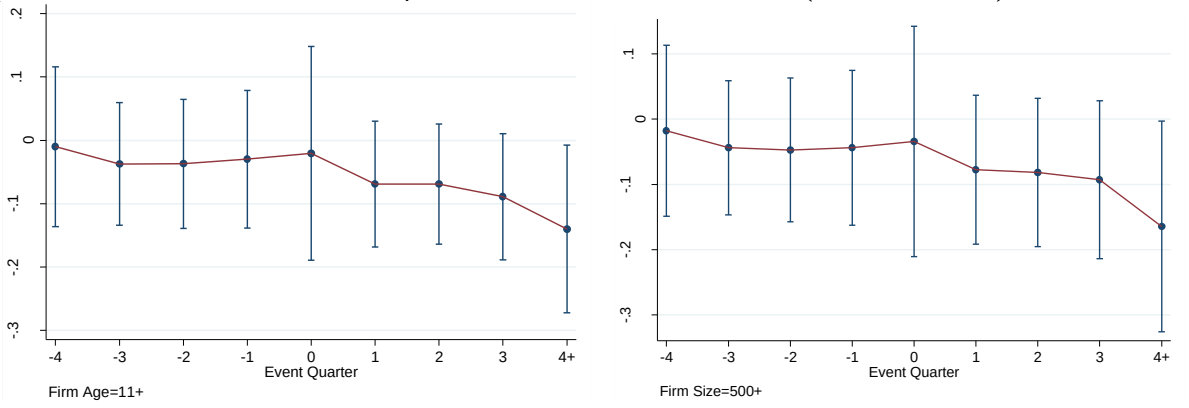


Table 4.5. Dynamic effects of security breach notification laws

	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
	Firm Age (Years since foundation)				Firm Size (# of Employees)			
	All Ages	0-3	4-10	11+	All sizes	0-49	50-499	500+
SBNL[0Q]	-0.034**	-0.028	-0.018	-0.040**	-0.037**	-0.014	-0.032	-0.018
	(0.016)	(0.045)	(0.040)	(0.018)	(0.018)	(0.017)	(0.033)	(0.067)
SBNL[1Q]	-0.036**	-0.034	-0.031	-0.038**	-0.040*	-0.020	-0.055	-0.060
	(0.018)	(0.052)	(0.041)	(0.018)	(0.020)	(0.018)	(0.034)	(0.038)
SBNL[2Q]	-0.038*	-0.060	-0.022	-0.038**	-0.043*	-0.020	-0.069*	-0.058
	(0.019)	(0.054)	(0.046)	(0.018)	(0.022)	(0.020)	(0.036)	(0.039)
SBNL[3Q]	-0.044*	-0.043	-0.033	-0.047**	-0.050*	-0.031	-0.048	-0.079*
	(0.022)	(0.079)	(0.045)	(0.021)	(0.026)	(0.023)	(0.035)	(0.044)
SBNL[4Q+]	-0.074**	-0.074	-0.038	-0.072**	-0.089*	-0.043	-0.125**	-0.150**
	(0.036)	(0.086)	(0.067)	(0.033)	(0.044)	(0.038)	(0.048)	(0.066)
Unemployment	-0.018**	-0.011	-0.001	-0.020*	-0.019**	-0.014*	-0.031	-0.023
	(0.009)	(0.018)	(0.015)	(0.011)	(0.009)	(0.007)	(0.019)	(0.019)
PI growth rate	0.341	0.220	0.410	0.431	0.259	0.093	0.011	-0.309
	(0.240)	(0.735)	(0.361)	(0.327)	(0.249)	(0.169)	(0.403)	(0.653)
Housing_Price	0.000	0.000	0.001	-0.000	0.000	0.001**	0.000	0.000
	(0.000)	(0.001)	(0.001)	(0.000)	(0.000)	(0.000)	(0.001)	(0.001)
State Fixed Effects	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Year-Quarter Fixed Effects	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Observations	3,358	3,358	3,358	3,358	3,358	3,358	3,358	3,358
R-squared	0.995	0.971	0.980	0.992	0.995	0.996	0.981	0.906

*Notes. Robust standard errors clustered by state are reported in parentheses. ***, **, and * denote significance at the 1%, 5%, and 10% level, respectively.* $SBNL[iQ]_{st}$ *is set to one if SBNL is effective i quarters before year-quarter t for state s, and zero otherwise. PI growth rate stands for personal income growth rate.*

Table 4.6. Placebo tests

	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
	Placebo Timing $= -12$		*Placebo Industry: Computers and Communications*					
VARIABLES	Firm Age =11+	Firm Size =500+	Firm Age 0-3	Firm Age 4-10	Firm Age 11+	Firm Size 0-49	Firm Size 50-499	Firm Size 500+
SBNL_Placeo	-0.077	-0.093						
	(0.051)	(0.060)						
SBNL			-0.074	-0.014	-0.011	-0.057	0.179**	0.052
			(0.124)	(0.139)	(0.057)	(0.052)	(0.086)	(0.087)
Unemployment	-0.026*	-0.022	0.008	0.026	-0.048**	-0.033	0.038	-0.097***
	(0.014)	(0.019)	(0.048)	(0.055)	(0.021)	(0.022)	(0.028)	(0.029)
Personal_Income_Growth	-0.222	-0.262	4.050**	0.408	-0.725	-0.607	2.008**	1.472
	(0.663)	(0.627)	(1.746)	(1.595)	(0.652)	(0.818)	(0.806)	(1.170)
Housing_Price	-0.000	0.000	-0.001	-0.002	-0.001	-0.002**	0.000	-0.009*
	(0.001)	(0.001)	(0.002)	(0.002)	(0.001)	(0.001)	(0.001)	(0.005)
State Fixed Effects	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Year-Quarter Fixed Effects	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Observations	3,358	3,358	2,863	3,058	3,367	3,291	3,194	3,361
R-squared	0.899	0.905	0.863	0.883	0.913	0.977	0.941	0.899

*Notes. Robust standard errors are reported in parentheses. ***, **, and * denote significance at the 1%, 5%, and 10% level, respectively. Placebo timing is set to be 12 quarters before the event quarter. See Table 2 for descriptions of the placebo industry.*

4.5 Discussions

With the continuous increase in digitization activities coinciding with the rise of cybersecurity threats and the cost of combating data breaches, a lingering question has been one related to whether or not complying with institutional pressures of addressing cybersecurity threats hinders digital growth. Through a natural experiment, this paper empirically measures the economic impact of the enactment of security breach notification laws toward IT service industries. By exploiting the staggered passages of SBNLs, we employ a difference-in-differences design to identify the effect of SBNL enactments on the employment of IT service providers. The results show that passages of SBNL significantly reduces employment for larger and more mature IT service providers, suggesting that digitization is slowed down by cybersecurity requirements.

Before discussing the implications of the study, we first acknowledge two limitations. First, inherent to the nature of DID design and limitations of aggregated data, the study does not provide explicit insights about the exact nature of employment dynamics in providers that cater to cybersecurity services versus those who don't. Our key argument is that SBNL enactment reduces the demand for general IT, thus reducing its supply, as reflected in the employment reduction in IT service providers. However, to directly measure the supply and demand of digitization, further firm-level scrutiny is required to better understand the nature of the overall decrease in IT service employment as a result of passing SBNLs.

The second limitation of the study is inherent to the broad unit of analysis, where we implicitly assumed different states are comparable without the SBNL shocks. This assumption can be challenged by comparing states with vastly different economic landscapes (e.g. New York and Wyoming). While we have controlled for three macro-economic variables, there are likely other uncontrolled covariates (e.g. the level of automation). To better address the issue, future studies with employment data on more granular geographic levels, e.g., the county level, can form a better selection of counterfactuals. While each state may not be entirely comparable, neighboring counties

along state borders are very similar communities, where they experience SBNL shocks at different points in time.

Despite the limitations, this study has two implications for the literature. First, it adds to the digital economics literature that has traditionally focused on cost reduction through digitization. This study quantifies an added cost of digitization, i.e., cybersecurity. The advancement of digitization has vastly reduced the cost to search for, replicate, and transport data (Goldfarb and Tucker 2019). While these lowered costs create countless benefits, they also increase the exposure of sensitive data. To mitigate the threats, policy-makers introduced SBNLs to stimulate cybersecurity initiatives by firms. However, we have found evidence that in order to avoid the compliance costs of SBNLs, firms are disincentivized to engage in digitization, as reflected by employment reduction in service providers of digitization. The digital economics literature is closely related to the IS field as IT adoption and IT investment are both tied with digitization. As such, this paper serves as a bridge between cybersecurity literature and the economics of digitization.

Second, this paper links cybersecurity with general IT. Behavioral security studies have addressed relationships between organizational risk mitigation mechanisms and psychological behavioral intentions (Bulgurcu et al. 2010; D'Arcy et al. 2009; Siponen and Vance 2010; Willison and Warkentin 2013). Organizational-level cybersecurity studies largely focus on risk mitigation through cybersecurity investments (Angst et al. 2017; Kwon and Johnson 2018), as well as the value of cybersecurity investments (Bose and Leung 2019; Gordon et al. 2010). State-level cybersecurity studies explore the effectiveness of cybersecurity legislation (Murciano-Goroff 2019; Romanosky et al. 2011). This study relates to these prior studies since state-level cybersecurity legislation affects firm-level cybersecurity initiatives, which in turn influence individual-level behavioral intentions. This paper differs from existing studies in that it focuses on the broader economic angle of cybersecurity. While digitization necessitates cybersecurity, we study how cybersecurity impacts the advancement of digitization on an aggregate level, through focusing on the important indicator of employment.

For policy-makers, this study reveals an unintended consequence of SBNLs. The current debates of SBNLs center on whether certain provisions in the laws are effective in mitigating data breaches, and whether there is a need for a federal-level SBNL. This study sheds light on these discussions by providing a view of the unintended aspects of this legislation. Understanding the economic consequences of well-intentioned legislative agendas that affect firm-level cybersecurity initiatives on a larger scale is pertinent to the progress and advancement of such legislation.

CHAPTER V: CONCLUSION

While cybersecurity continues to pose threats to organizations, one of the biggest challenges for organizations is to justify cybersecurity investment as "a strategic investment in reduction of corporate risk, and a positive contribution to the realization of business value."[21] To this end, we document the business values of internal (infrastructural) and external (innovation-oriented) cybersecurity investments in the first two essays, respectively. In the first essay, we find that the value of infrastructural cybersecurity investments is best leveraged through complementary investments in cybersecurity labor and evaluated within a socially relative framework. We also reveal the reduction of cost of capital as one avenue for business value creation. In essay 2, we find that an innovation-oriented (forward-looking) cybersecurity investments (CVC) also contributes to firm values, especially for IT firms in more recent years. Together, the two essays provide a complementary picture of internal and external cybersecurity investments.

Moving beyond the micro-underpinnings of cybersecurity in organizations, we study the broader impact of cybersecurity toward general IT. Apart from increased spending in cybersecurity, another (related) trend in cybersecurity is the more stringent regulatory environment in cybersecurity. In championing these regulations to mitigate cyber threats, it is important to quantify the unintended economic consequences of well-intentioned regulations, so that policy-makers can make more informed decisions. In essay 3, we find that enactments of security breach notification laws reduce employment in large and mature IT service firms, suggesting that cybersecurity laws can have a negative impact toward the digital economy.

While the three essays cover a wide range of topics in cybersecurity, they are inherently linked by the fact that infrastructural cybersecurity investments are closely related to innovations

[21] https://www.csoonline.com/article/3438321/three-strategies-to-prove-securitys-value.html

in cybersecurity, both of which are often instigated by cybersecurity legislation. Overall, the essays document the value of cybersecurity investments and the cost of cybersecurity legislation. In doing so, the dissertation covers a wide range of institutional entities that both shape and are impacted by the cybersecurity ecosystem.

The dissertation contributes to several streams of literature. Essay 1 and 2 add to the studies on the business value of cybersecurity investment. While the preventive value of cybersecurity investment is well-documented, particularly in the healthcare industry (Kwon and Johnson 2013; Kwon and Johnson 2014), the bottom-line value measured by more tangible accounting indices and the value-creation mechanism are not clear. Essay 1 connects cybersecurity to the book-keeping indices of sustained performance, ties them into the deeper strategic efforts of talent acquisition in competitive markets, makes them relevant to the institutional positioning of a firm relative to its peers, and positions them as a significant factor in connecting to stakeholders and accessing competitive sources of financing. It also echoes recent studies on the preventive value of cybersecurity investments by linking talent recruitment with substantive cybersecurity investments (Angst et al. 2017; Kwon and Johnson 2018).

Essay 2 adds to the business value of cybersecurity investment literature by revealing the value of innovation in cybersecurity as an area that is predominantly believed to be costly but not value-generating. More generally, it also contributes to the business value of IT literature, where the main focus has been on infrastructural and talent investments (Brynjolfsson and Hitt 1996; Tambe and Hitt 2012) and the value of investments in IT innovation is understudied.

Finally, essay 3 adds to the digital economics literature by revealing cybersecurity as an inherent economic cost attached to digitization, in contrast to the well-documented cost reduction nature of going digital (Goldfarb and Tucker 2019). Essay 3 also contributes to the cybersecurity literature by linking cybersecurity with general IT. While existing cybersecurity literature largely focuses on the micro-underpinning of individual behavior and organizational initiatives related to the effectiveness

of cybersecurity practices, we broaden the picture by investigating how cybersecurity impacts general IT.

The dissertation also has immediate implications for practitioners. As security executives struggle to tie cybersecurity to companies' general IT strategy and justifying the cost of cybersecurity spending (with no direct contribution to companies' revenue), we provide empirical evidence on the magnitude of the business value and the channels through which cybersecurity values are created. We also point to the value of investing in forward-looking, innovation-oriented cybersecurity. For policymakers of cybersecurity laws, apart from considering the effectiveness in mitigating cyber threats, we have shown that the unintended economic consequences of cybersecurity legislation should also be included in the debate. As more privacy and security laws are introduced on the state and federal level and spending in cybersecurity continue to grow, our studies provide some baseline evidence for corporate executives and legislators in their practices.

REFERENCES

Accenture. 2017. "Cost of Cyber Crime Study: Insights on the Security Investments That Make a Difference."

Acquisti, A., Friedman, A., and Telang, R. 2006. "Is There a Cost to Privacy Breaches? An Event Study," *27th International Conference on Information Systems*, Milwaukee, Wisconsin, pp. 1563-1580.

Amir, E., Levi, S., and Livne, T. 2018. "Do Firms Underreport Information on Cyber-Attacks? Evidence from Capital Markets," *Review of Accounting Studies* (23:3), pp. 1-30.

Angrist, J., and Pischke, J.-S. 2009. *Mostly Harmless Econometrics: An Empiricist's Companion*. Princeton University Press.

Angst, C. M., Block, E. S., D'arcy, J., and Kelley, K. 2017. "When Do It Security Investments Matter? Accounting for the Influence of Institutional Factors in the Context of Healthcare Data Breaches," *MIS Quarterly* (41:3), pp. 893-916.

Appel, I., Farre-Mensa, J., and Simintzi, E. 2019. "Patent Trolls and Startup Employment," *Journal of Financial Economics* (133:3), pp. 708-725.

Aral, S., Bakos, Y., and Brynjolfsson, E. 2017. "Information Technology, Repeated Contracts, and the Number of Suppliers," *Management Science* (64:2), pp. 592-612.

Argote, L., and Greve, H. R. 2007. "A Behavioral Theory of the Firm—40 Years and Counting: Introduction and Impact," *Organization Science* (18:3), pp. 337-349.

Arthur, M. M. 2003. "Share Price Reactions to Work-Family Initiatives: An Institutional Perspective," *Academy of Management Journal* (46:4), pp. 497-505.

Ashraf, M., and Sunder, J. 2018. "Mandatory Disclosure of Cyber Incidents and the Cost of Equity."

Baker, L. B. 2018. "Under Threat: Cyber Security Startups Fall on Harder Times." from https://www.reuters.com/article/us-cybersecurity-startups-analysis/under-threat-cyber-security-startups-fall-on-harder-times-idUSKBN1F62RW

Bansal, P., and Roth, K. 2000. "Why Companies Go Green: A Model of Ecological Responsiveness," *Academy of Management Journal* (43:4), pp. 717-736.

Baum, J. A., Rowley, T. J., Shipilov, A. V., and Chuang, Y.-T. 2005. "Dancing with Strangers: Aspiration Performance and the Search for Underwriting Syndicate Partners," *Administrative Science Quarterly* (50:4), pp. 536-575.

Belsis, P., Kokolakis, S., and Kiountouzis, E. 2005. "Information Systems Security from a Knowledge Management Perspective," *Information Management & Computer Security* (13:3), pp. 189-202.

Benaroch, M. 2018. "Real Options Models for Proactive Uncertainty-Reducing Mitigations and Applications in Cybersecurity Investment Decision Making," *Information Systems Research*).

Benaroch, M., and Kauffman, R. J. 2000. "Justifying Electronic Banking Network Expansion Using Real Options Analysis," *MIS quarterly* (24:2), pp. 197-225.

Benson, D., and Ziedonis, R. H. 2009. "Corporate Venture Capital as a Window on New Technologies: Implications for the Performance of Corporate Investors When Acquiring Startups," *Organization Science* (20:2), pp. 329-351.

Benson, D., and Ziedonis, R. H. 2010. "Corporate Venture Capital and the Returns to Acquiring Portfolio Companies," *Journal of Financial Economics* (98:3), pp. 478-499.

Bertrand, M., and Mullainathan, S. 2003. "Enjoying the Quiet Life? Corporate Governance and Managerial Preferences," *Journal of Political Economy* (111:5), pp. 1043-1075.
Bharadwaj, A. S., Bharadwaj, S. G., and Konsynski, B. R. 1999. "Information Technology Effects on Firm Performance as Measured by Tobin's Q," *Management Science* (45:7), pp. 1008-1024.
Bitektine, A., and Haack, P. 2015. "The "Macro" and the "Micro" of Legitimacy: Toward a Multilevel Theory of the Legitimacy Process," *Academy of Management Review* (40:1), pp. 49-75.
Bloom, N., and Van Reenen, J. 2002. "Patents, Real Options and Firm Performance," *The Economic Journal* (112:478).
Bose, I., and Leung, A. C. M. 2013. "The Impact of Adoption of Identity Theft Countermeasures on Firm Value," *Decision Support Systems* (55:3), pp. 753-763.
Bose, I., and Leung, A. C. M. 2019. "Adoption of Identity Theft Countermeasures and Its Short-and Long-Term Impact on Firm Value," *MIS Quarterly* (43:1), pp. 313-327.
Bravo-Biosca, A., Criscuolo, C., and Menon, C. 2016. "What Drives the Dynamics of Business Growth?," *Economic Policy* (31:88), pp. 703-742.
Brynjolfsson, E., and Hitt, L. 1996. "Paradox Lost? Firm-Level Evidence on the Returns to Information Systems Spending," *Management Science* (42:4), pp. 541-558.
Bulgurcu, B., Cavusoglu, H., and Benbasat, I. 2010. "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness," *MIS quarterly* (34:3), pp. 523-548.
Cachon, G. P., Gallino, S., and Olivares, M. 2018. "Does Adding Inventory Increase Sales? Evidence of a Scarcity Effect in Us Automobile Dealerships," *Management Science* (65:4), pp. 1469-1485.
Campbell, K., Gordon, L. A., Loeb, M. P., and Zhou, L. 2003. "The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market," *Journal of Computer Security* (11:3), pp. 431-448.
Cavusoglu, H., Mishra, B., and Raghunathan, S. 2004. "The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers," *International Journal of Electronic Commerce* (9:1), pp. 70-104.
Cavusoglu, H., Raghunathan, S., and Yue, W. T. 2008. "Decision-Theoretic and Game-Theoretic Approaches to It Security Investment," *Journal of Management Information Systems* (25:2), pp. 281-304.
Ceccagnoli, M., Higgins, M. J., and Kang, H. D. 2017. "Corporate Venture Capital as a Real Option in the Markets for Technology," *Technology & Engineering Management Conference (TEMSCON), 2017 IEEE*: IEEE, pp. 40-46.
Chai, S., Kim, M., and Rao, H. R. 2011. "Firms' Information Security Investment Decisions: Stock Market Evidence of Investors' Behavior," *Decision Support Systems* (50:4), pp. 651-661.
Chan, J., and Ghose, A. 2013. "Internet's Dirty Secret: Assessing the Impact of Online Intermediaries on Hiv Transmission," *MIS Quarterly* (38:4), pp. 955-976.
Chan, J., Mojumder, P., and Ghose, A. 2019. "The Digital Sin City: An Empirical Study of Craigslist's Impact on Prostitution Trends," *Information Systems Research* (30:1), pp. 219-238.
Chari, M. D., Devaraj, S., and David, P. 2008. "Research Note—the Impact of Information Technology Investments and Diversification Strategies on Firm Performance," *Management Science* (54:1), pp. 224-234.
Chemmanur, T. J., Loutskina, E., and Tian, X. 2014. "Corporate Venture Capital, Value Creation, and Innovation," *The Review of Financial Studies* (27:8), pp. 2434-2473.
Chesbrough, H. 2000. "Designing Corporate Ventures in the Shadow of Private Venture Capital," *California Management Review* (42:3), pp. 31-49.
Cochran, P. L., and Wood, R. A. 1984. "Corporate Social Responsibility and Financial Performance," *Academy of Management Journal* (27:1), pp. 42-56.

Cohen, J. B., Black, F., and Scholes, M. 1972. "The Valuation of Option Contracts and a Test of Market Efficiency," *The Journal of Finance* (27:2), pp. 399-417.
Coma, C. W., and Douglas, P. H. 1928. "A Theory of Production," *Proceedings of the Fortieth Annual Meeting of the American Economic Association*, p. 165.
Cremonini, M., and Nizovtsev, D. 2009. "Risks and Benefits of Signaling Information System Characteristics to Strategic Attackers," *Journal of Management Information Systems* (26:3), pp. 241-274.
Cyert, R. M., and March, J. G. 1963. *A Behavioral Theory of the Firm*. Englewood Cliffs, NJ: Prentice Hall.
D'Arcy, J., Hovav, A., and Galletta, D. 2009. "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach," *Information Systems Research* (20:1), pp. 79-98.
DiMaggio, P., and Powell, W. W. 1983. "The Iron Cage Revisited: Collective Rationality and Institutional Isomorphism in Organizational Fields," *American Sociological Review* (48:2), pp. 147-160.
Dimov, D., and De Clercq, D. 2006. "Venture Capital Investment Strategy and Portfolio Failure Rate: A Longitudinal Study," *Entrepreneurship Theory and Practice* (30:2), pp. 207-223.
Dixit, A. K., and Pindyck, R. S. 1994. *Investment under Uncertainty*. Princeton university press.
Doh, J. P., Howton, S. D., Howton, S. W., and Siegel, D. S. 2010. "Does the Market Respond to an Endorsement of Social Responsibility? The Role of Institutions, Information, and Legitimacy," *Journal of Management* (36:6), pp. 1461-1485.
Dushnitsky, G., and Lenox, M. J. 2005a. "When Do Firms Undertake R&D by Investing in New Ventures?," *Strategic Management Journal* (26:10), pp. 947-965.
Dushnitsky, G., and Lenox, M. J. 2005b. "When Do Incumbents Learn from Entrepreneurial Ventures?: Corporate Venture Capital and Investing Firm Innovation Rates," *Research Policy* (34:5), pp. 615-639.
Dushnitsky, G., and Lenox, M. J. 2006. "When Does Corporate Venture Capital Investment Create Firm Value?," *Journal of Business Venturing* (21:6), pp. 753-772.
Ernst, H., Witt, P., and Brachtendorf, G. 2005. "Corporate Venture Capital as a Strategy for External Innovation: An Exploratory Empirical Study," *R&D Management* (35:3), pp. 233-242.
Felin, T., and Hesterly, W. S. 2007. "The Knowledge-Based View, Nested Heterogeneity, and New Value Creation: Philosophical Considerations on the Locus of Knowledge," *Academy of Management Review* (32:1), pp. 195-218.
Fichman, R. G. 2004. "Real Options and It Platform Adoption: Implications for Theory and Practice," *Information systems research* (15:2), pp. 132-154.
Ginzel, L. E., Kramer, R. M., and Sutton, R. I. 1993. "Organizational Impression Management as a Reciprocal Influence Process: The Neglected Role of the Organizational Audience," *Research in Organizational Behavior* (15), pp. 227-227.
Goldfarb, A., and Tucker, C. 2019. "Digital Economics," *Journal of Economic Literature* (57:1), pp. 3-43.
Gordon, L. A., Loeb, M. P., and Lucyshyn, W. 2003. "Information Security Expenditures and Real Options: A Wait-and-See Approach," *Computer Security Journal* (19:2), pp. 1-7.
Gordon, L. A., Loeb, M. P., and Sohail, T. 2010. "Market Value of Voluntary Disclosures Concerning Information Security," *MIS Quarterly* (34:3), pp. 567-594.
Gordon, L. A., Loeb, M. P., and Zhou, L. 2011. "The Impact of Information Security Breaches: Has There Been a Downward Shift in Costs?," *Journal of Computer Security* (19:1), pp. 33-56.
Greve, H. R. 2003a. "A Behavioral Theory of R&D Expenditures and Innovations: Evidence from Shipbuilding," *Academy of Management Journal* (46:6), pp. 685-702.
Greve, H. R. 2003b. *Organizational Learning from Performance Feedback: A Behavioral Perspective on Innovation and Change*. Cambridge University Press.

Haislip, J., Kolev, K., Pinsker, R., and Steffen, T. 2019. "The Economic Cost of Cybersecurity Breaches: A Broad-Based Analysis," in: *Workshop on the Economics of Information Security*. Boston, MA.
Haltiwanger, J., Hathaway, I., and Miranda, J. 2014. "Declining Business Dynamism in the Us High-Technology Sector."
Haswell, S., and Holmes, S. 1989. "Estimating the Small Business Failure Rate: A Reappraisal," *Journal of Small Business Management* (27:3), p. 68.
Havakhor, T., and Sabherwal, R. 2018. "Organizational Investment in New It Ventures: Evidence from Big Data Ventures."
Havakhor, T., Zhang, T., and Hammer, B. 2018. "The Business Value of Engaging in Counter-Breach Initiatives," *Americas Conference on Information Systems*, New Orleans.
Herath, H. S., and Herath, T. C. 2008. "Investments in Information Security: A Real Options Perspective with Bayesian Postaudit," *Journal of Management Information Systems* (25:3), pp. 337-375.
Ho, J., Tian, F., Wu, A., and Xu, S. X. 2017. "Seeking Value through Deviation? Economic Impacts of It Overinvestment and Underinvestment," *Information Systems Research* (28:4), pp. 850-862.
Hui, K.-L., Kim, S. H., and Wang, Q.-H. 2017. "Cybercrime Deterrence and International Legislation: Evidence from Distributed Denial of Service Attacks," *MIS Quarterly* (41:2), p. 497.
Iyer, D. N., and Miller, K. D. 2008. "Performance Feedback, Slack, and the Timing of Acquisitions," *Academy of Management Journal* (51:4), pp. 808-822.
Jeong, C. Y., and Lee, S.-Y. T. 2019. "Information Security Breaches and It Security Investments: Impacts on Competitors," *Information & Management* (56:5), pp. 681-695.
Kankanhalli, A., Teo, H.-H., Tan, B. C., and Wei, K.-K. 2003. "An Integrative Study of Information Systems Security Effectiveness," *International Journal of Information Management* (23:2), pp. 139-154.
Karnani, A. 2011. "'Doing Well by Doing Good': The Grand Illusion," *California Management Review* (53:2), pp. 69-86.
Kerr, W. R., Nanda, R., and Rhodes-Kropf, M. 2014. "Entrepreneurship as Experimentation," *Journal of Economic Perspectives* (28:3), pp. 25-48.
King, A. A., and Shaver, J. M. 2001. "Are Aliens Green? Assessing Foreign Establishments' Environmental Conduct in the United States," *Strategic Management Journal* (22:11), pp. 1069-1085.
Kostova, T., and Zaheer, S. 1999. "Organizational Legitimacy under Conditions of Complexity: The Case of the Multinational Enterprise," *Academy of Management Review* (24:1), pp. 64-81.
Kvochko, E., and Pant, R. 2015. "Why Data Breaches Don't Hurt Stock Prices," in: *Harvard Business Review*.
Kwon, J., and Johnson, M. E. 2013. "Health-Care Security Strategies for Data Protection and Regulatory Compliance," *Journal of Management Information Systems* (30:2), pp. 41-66.
Kwon, J., and Johnson, M. E. 2014. "Proactive Versus Reactive Security Investments in the Healthcare Sector," *MIS Quarterly* (38:2), pp. 451-471.
Kwon, J., and Johnson, M. E. 2018. "Meaningful Healthcare Security: Does Meaningful-Use Attestation Improve Information Security Performance?," *MIS Quarterly* (42:4), pp. 1043-1067.
Leeson, P. T., and Coyne, C. J. 2005. "The Economics of Computer Hacking," *Journal of Law, Economics and Policy* (1:2), pp. 511-532.
Lemmon, M. L., and Zender, J. F. 2019. "Asymmetric Information, Debt Capacity, and Capital Structure," *Journal of Financial and Quantitative Analysis* (54:1), pp. 31-59.
Levitt, B., and March, J. G. 1988. "Organizational Learning," *Annual Review of Sociology* (14:1), pp. 319-338.

Lu, S. F., Rui, H., and Seidmann, A. 2017. "Does Technology Substitute for Nurses? Staffing Decisions in Nursing Homes," *Management Science* (64:4), pp. 1842-1859.
Ma, S. 2019. "The Life Cycle of Corporate Venture Capital," *Review of Financial Studies* (Forthcoming).
McGrath, R. G. 1997. "A Real Options Logic for Initiating Technology Positioning Investments," *Academy of management review* (22:4), pp. 974-996.
McGrath, R. G. 1999. "Falling Forward: Real Options Reasoning and Entrepreneurial Failure," *Academy of Management review* (24:1), pp. 13-30.
McGrath, R. G., Ferrier, W. J., and Mendelow, A. L. 2004. "Real Options as Engines of Choice and Heterogeneity," *Academy of Management Review* (29:1), pp. 86-101.
McWilliams, A., and Siegel, D. 2001. "Corporate Social Responsibility: A Theory of the Firm Perspective," *Academy of Management Review* (26:1), pp. 117-127.
Melville, N., Kraemer, K., and Gurbaxani, V. 2004. "Information Technology and Organizational Performance: An Integrative Model of It Business Value," *MIS Quarterly* (28:2), pp. 283-322.
Miller, A. R., and Tucker, C. 2009. "Privacy Protection and Technology Diffusion: The Case of Electronic Medical Records," *Management Science* (55:7), pp. 1077-1093.
Miller, D., and Chen, M.-J. 1994. "Sources and Consequences of Competitive Inertia: A Study of the Us Airline Industry," *Administrative Science Quarterly* (39:1), pp. 1-23.
Mitchell, R. K., Agle, B. R., and Wood, D. J. 1997. "Toward a Theory of Stakeholder Identification and Salience: Defining the Principle of Who and What Really Counts," *Academy of Management Review* (22:4), pp. 853-886.
Mithas, S., and Rust, R. T. 2016. "How Information Technology Strategy and Investments Influence Firm Performance: Conjecture and Empirical Evidence," *MIS Quarterly* (40:1), pp. 223-245.
Murciano-Goroff, R. 2019. "Do Data Breach Disclosure Laws Increase Firms' Investment in Securing Their Digital Infrastructure?," *Workshop on the Economics of Information Security*, Boston, MA.
Nohria, N., and Gulati, R. 1996. "Is Slack Good or Bad for Innovation?," *Academy of Management Journal* (39:5), pp. 1245-1264.
Park, H. D., and Steensma, H. K. 2012. "When Does Corporate Venture Capital Add Value for New Ventures?," *Strategic Management Journal* (33:1), pp. 1-22.
Peterson, B. 2017. "Cybersecurity Is a $81.7 Billion Market - and Startups Are Raking in the Dough." from http://www.businessinsider.com/cybersecurity-startups-are-hot-and-investors-are-taking-notice-2017-7
Peterson, B. 2018. "Cybersecurity Startups Raked in $7.6 Billion in Vc Money in 2017 - Twice as Much as the Year Before." from http://www.businessinsider.com/cybersecurity-startups-raked-in-76-billion-in-vc-money-in-2017-2018-1
Pettit, D. 2018. "Wsj Top 25 Tech Companies to Watch 2018." from https://www.wsj.com/articles/wsj-top-25-tech-companies-to-watch-2018-1528825018
Ransbotham, S., and Mitra, S. 2009. "Choice and Chance: A Conceptual Model of Paths to Information Security Compromise," *Information Systems Research* (20:1), pp. 121-139.
Ransbotham, S., and Mitra, S. 2010. "Target Age and the Acquisition of Innovation in High-Technology Industries," *Management Science* (56:11), pp. 2076-2093.
Robins, J., and Wiersema, M. F. 1995. "A Resource ‐ Based Approach to the Multibusiness Firm: Empirical Analysis of Portfolio Interrelationships and Corporate Financial Performance," *Strategic Management Journal* (16:4), pp. 277-299.
Rogers, J. L., Van Buskirk, A., and Zechman, S. L. 2011. "Disclosure Tone and Shareholder Litigation," *The Accounting Review* (86:6), pp. 2155-2183.
Romanosky, S., Telang, R., and Acquisti, A. 2011. "Do Data Breach Disclosure Laws Reduce Identity Theft?," *Journal of Policy Analysis and Management* (30:2), pp. 256-286.

Santhanam, R., and Hartono, E. 2003. "Issues in Linking Information Technology Capability to Firm Performance," *MIS Quarterly* (27:1), pp. 125-153.
Schwartz, E. S., and Zozaya-Gorostiza, C. 2003. "Investment under Uncertainty in Information Technology: Acquisition and Development Projects," *Management Science* (49:1), pp. 57-70.
Sen, R. 2018. "Challenges to Cybersecurity: Current State of Affairs," *Communications of the Association for Information Systems* (43:1), pp. 22-44.
Sen, R., and Borle, S. 2015. "Estimating the Contextual Risk of Data Breach: An Empirical Approach," *Journal of Management Information Systems* (32:2), pp. 314-341.
Sharfman, M. P., and Fernando, C. S. 2008. "Environmental Risk Management and the Cost of Capital," *Strategic Management Journal* (29:6), pp. 569-592.
Shear, M. D., and Singer, N. 2015. "Obama to Call for Laws Covering Data Hacking and Student Privacy," in: *New York Times*.
Sieberg, D. 2005. "Hackers Shift Focus to Financial Gain," in: *CNN*.
Siponen, M., and Vance, A. 2010. "Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations," *MIS quarterly* (34:3), pp. 487-502.
Stock, J. H., and Yogo, M. 2005. "Testing for Weak Instruments in Linear Iv Regression," in *Identification and Inference for Econometric Models*, D.W.K. Andrews and J.H. Stock (eds.). Cambridge, UK: Cambridge University Press, pp. 80–108.
Straub, D. W. 1990. "Effective Is Security: An Empirical Study," *Information Systems Research* (1:3), pp. 255-276.
Suchman, M. C. 1995. "Managing Legitimacy: Strategic and Institutional Approaches," *Academy of Management Review* (20:3), pp. 571-610.
Suddaby, R., and Greenwood, R. 2005. "Rhetorical Strategies of Legitimacy," *Administrative Science Quarterly* (50:1), pp. 35-67.
Sykes, H. B. 1986. "The Anatomy of a Corporate Venturing Program: Factors Influencing Success," *Journal of Business Venturing* (1:3), pp. 275-293.
Tambe, P. 2014. "Big Data Investment, Skills, and Firm Value," *Management Science* (60:6), pp. 1452-1469.
Tambe, P., and Hitt, L. M. 2012. "The Productivity of Information Technology Investments: New Evidence from It Labor Data," *Information Systems Research* (23:3-part-1), pp. 599-617.
Tambe, P., and Hitt, L. M. 2013. "Job Hopping, Information Technology Spillovers, and Productivity Growth," *Management Science* (60:2), pp. 338-355.
Taudes, A., Feurstein, M., and Mild, A. 2000. "Options Analysis of Software Platform Decisions: A Case Study," *MIS quarterly* (24:2), pp. 227-243.
Tong, T. W., and Li, Y. 2011. "Real Options and Investment Mode: Evidence from Corporate Venture Capital and Acquisition," *Organization Science* (22:3), pp. 659-674.
Trigeorgis, L. 1993. "Real Options and Interactions with Financial Flexibility," *Financial management* (22:3), pp. 202-224.
Von Solms, R., and Van Niekerk, J. 2013. "From Information Security to Cyber Security," *Computers & Security* (38), pp. 97-102.
Wadhwa, A., and Kotha, S. 2006. "Knowledge Creation through External Venturing: Evidence from the Telecommunications Equipment Manufacturing Industry," *Academy of Management Journal* (49:4), pp. 819-835.
Wang, J., Chaudhury, A., and Rao, H. R. 2008. "Research Note—a Value-at-Risk Approach to Information Security Investment," *Information Systems Research* (19:1), pp. 106-120.
Wang, T., Kannan, K. N., and Ulmer, J. R. 2013. "The Association between the Disclosure and the Realization of Information Security Risk Factors," *Information Systems Research* (24:2), pp. 201-218.
Willison, R., and Warkentin, M. 2013. "Beyond Deterrence: An Expanded View of Employee Computer Abuse," *MIS quarterly* (37:1), pp. 1-20.

Wu, L., Hitt, L., and Lou, B. 2019. "Data Analytics Skills, Innovation and Firm Productivity," *Management Science* (Forthcoming).

Xue, L., Ray, G., and Sambamurthy, V. 2012. "Efficiency or Innovation: How Do Industry Environments Moderate the Effects of Firms' It Asset Portfolios?," *MIS Quarterly* (36:2), pp. 509-528.

Zadelhoff, M. v. 2017. "Cybersecurity Has a Serious Talent Shortage. Here's How to Fix It," in: *Harvard Business Review*.

Zajac, E. J., and Westphal, J. D. 2004. "The Social Construction of Market Value: Institutionalization and Learning Perspectives on Stock Market Reactions," *American Sociological Review* (69:3), pp. 433-457.

APPENDICES

Appendix A: Keywords List

Table A1. Keywords Used to Search for Data Breaches and Cybersecurity investments and to Train the Machine Learning Algorithm used to Identify Skillsets

Data Breaches and Cybersecurity Investments	Cybersecurity Skillsets
security	risk management
computer security	cybersecurity
breach	cyber
security breach	cyber defense
information security breach	incident response
privacy	vulnerability assessment
threat	threat analysis
attack	exploitation analysis
protect	cyber operation
protection	cyber investigation
vulnerability	digital forensics
cyber attack	authentication
computer break-in	compliance
break-in	assurance
computer attack	security
network intrusion	protect
data theft	incident
identity theft	firewall
phishing	confidentiality
hacker	integrity
computer virus	availability
cyber fraud	access control
denial of service	cyberspace
	defense
	Security assessment

Appendix B: First Stage of 2SLS Estimation

	SS1: Under-performing firms			SS2: On-par firms (high risk)			SS3: On-par firms (low risk)			SS4: Over-performing firms		
DV=	PECIs	TR	TR*PECIs	PECIs	TR	TR*PECIs	PECIs	TR	TR*PECIs	PECIs	TR	TR*PECIs
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)
ex_IT	0.302***	0.334***	0.326***	0.332***	0.329***	0.317***	0.308***	0.299***	0.323***	0.323***	0.314***	0.334***
	(0.059)	(0.061)	(0.074)	(0.074)	(0.071)	(0.056)	(0.075)	(0.061)	(0.083)	(0.052)	(0.066)	(0.072)
ind_IT	0.089**	0.085**	0.093***	0.089**	0.084**	0.091**	0.093***	0.084**	0.089**	0.091**	0.084**	0.093***
	(0.031)	(0.027)	(0.025)	(0.034)	(0.032)	(0.033)	(0.016)	(0.027)	(0.033)	(0.031)	(0.026)	(0.016)
Tax	-0.033*	-0.034*	-0.032*	-0.034*	-0.032*	-0.032*	-0.03*	-0.032*	-0.031*	-0.031*	-0.031*	-0.033*
	(0.014)	(0.017)	(0.016)	(0.016)	(0.014)	(0.016)	(0.013)	(0.014)	(0.014)	(0.013)	(0.013)	(0.014)
Surplus	0.127***	0.138***	0.126***	0.131***	0.132***	0.143***	0.129***	0.133***	0.138***	0.127***	0.125***	0.138***
	(0.027)	(0.021)	(0.025)	(0.02)	(0.027)	(0.022)	(0.021)	(0.022)	(0.026)	(0.023)	(0.026)	(0.04)
MER	0.005	0.006	0.006	0.006	0.006	0.005	0.006	0.006	0.005	0.006	0.005	0.005
	(0.004)	(0.004)	(0.005)	(0.004)	(0.005)	(0.004)	(0.004)	(0.004)	(0.004)	(0.005)	(0.003)	(0.004)
SER	0.016#	0.015#	0.016#	0.016#	0.015#	0.015#	0.015#	0.016#	0.016#	0.016#	0.016#	0.015#
	(0.008)	(0.008)	(0.009)	(0.008)	(0.009)	(0.009)	(0.008)	(0.009)	(0.009)	(0.009)	(0.009)	(0.009)
IEX	-0.011	-0.011	-0.01	-0.011	-0.011	-0.011	-0.011	-0.011	-0.011	-0.011	-0.011	-0.01
	(0.009)	(0.01)	(0.006)	(0.009)	(0.009)	(0.009)	(0.009)	(0.007)	(0.008)	(0.007)	(0.009)	(0.006)
Avg PECIs	0.494***	0.215***	0.356***	0.512***	0.236***	0.36***	0.512***	0.228***	0.373***	0.494***	0.219***	0.373***
	(0.094)	(0.046)	(0.084)	(0.12)	(0.066)	(0.062)	(0.088)	(0.042)	(0.063)	(0.112)	(0.036)	(0.056)
Avg TR	0.229***	0.485***	0.299***	0.238***	0.49***	0.296***	0.244***	0.504***	0.316***	0.225***	0.513***	0.321***
	(0.039)	(0.076)	(0.045)	(0.045)	(0.102)	(0.074)	(0.067)	(0.104)	(0.059)	(0.046)	(0.139)	(0.049)
Avg TR * Avg PECIs	0.392***	0.36***	0.432***	0.36***	0.36***	0.416***	0.399***	0.364***	0.424***	0.399***	0.357***	0.449***
	(0.081)	(0.106)	(0.081)	(0.065)	(0.103)	(0.074)	(0.111)	(0.093)	(0.065)	(0.107)	(0.055)	(0.133)
SBNL	0.444***	0.427***	0.453***	0.435***	0.468***	0.473***	0.444***	0.435***	0.427***	0.444***	0.435***	0.432***
	(0.108)	(0.121)	(0.088)	(0.087)	(0.108)	(0.114)	(0.093)	(0.083)	(0.127)	(0.075)	(0.105)	(0.118)
CyberDeg	0.298***	0.324***	0.206***	0.336***	0.333***	0.208***	0.315***	0.327***	0.217***	0.336***	0.304***	0.217***
	(0.072)	(0.049)	(0.035)	(0.079)	(0.056)	(0.041)	(0.085)	(0.091)	(0.043)	(0.06)	(0.078)	(0.054)
Firm controls	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES
Adj. R-Squared	0.68	0.72	0.63	0.71	0.62	0.68	0.72	0.73	0.64	0.59	0.64	0.67
Observations		884			718			992			606	

Notes. *PECIs stands for publicly emphasizing cybersecurity investments, TR for talent recruitment, ex_IT for previous year IT investment, ind_IT for industry IT investment, Tax for industry tax ratio, Surplus for the industry-operating surplus, MER for the industry material-energy input ratio, SER for the industry service-energy input ratio, IEX for the industry import-export value, SBNL for security breach notification law passage. Standard errors are in parentheses. ***p < 0.001; **p < 0.01; *p < 0.05; # p < 0.10.*

Appendix C: WACC Estimation

The firm's after-tax weighted average cost of capital (r_{WACC}) is expressed as:

$$r_{WACC} = (\frac{E}{E+D}).r_E + (\frac{D}{E+D}).r_D.(1\text{-T})$$

where E is the market value of firm equity, D is the market value of the firm's debt, r_e is the firm's cost of equity capital, r_D is the firm's cost of debt capital (retrieved from Bloomberg Financial), and T is the firm's rate of corporate taxation. r_E is the expected return from holding the firm's equity using a Capital Asset Pricing Model (CAPM) (Lintner 1975):

$$r_E = r_F + \beta_E.(r_M - r_F)$$

where r_F is the risk-free rate of investment (10-year US treasury bond rate), r_M, is the return on the market portfolio, and β_E is the firm's systematic risk ($\frac{Cov(r_M,\ r_F)}{Var(r_M)}$), estimated from COMPUSTAT.

References

Lintner, J. 1965, "The Valuation of Risk Assets and the Selection of Risky Investments in Stock Portfolios and Capital Budgets: A Reply," *The Review of Economics and Statistics* (47:1), pp. 13-37.

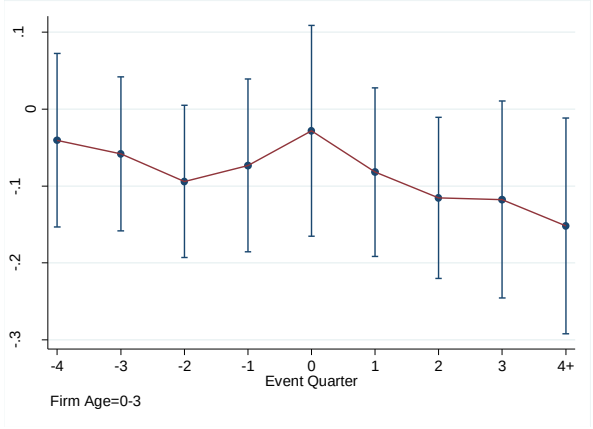
Appendix D: Exogeneity check using OLS

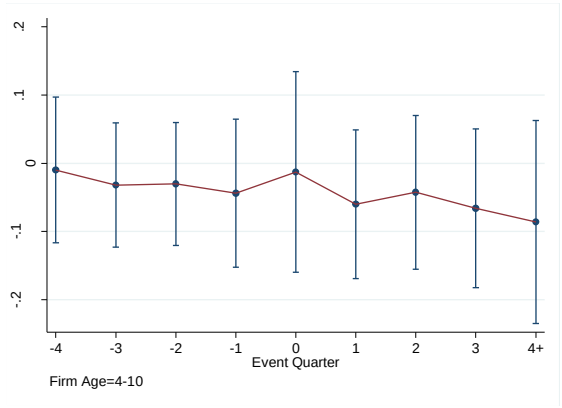
Table D1. OLS regressions (linear probability model)

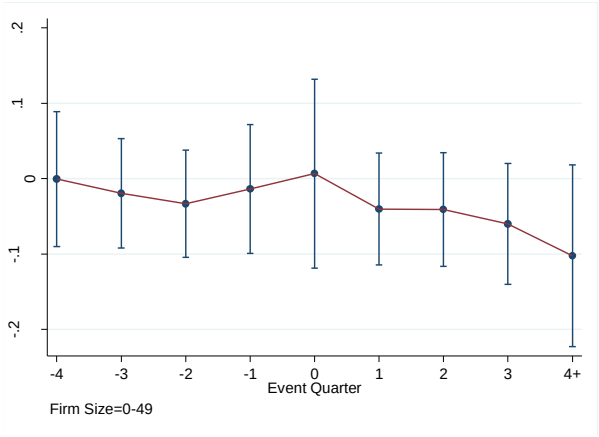
DV=SBNL	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
Unemployment Rate	0.000	0.004	-0.001	0.002	0.001	0.000	0.001	-0.000
	(0.004)	(0.010)	(0.003)	(0.013)	(0.003)	(0.012)	(0.003)	(0.012)
Personal Income Growth	-0.305	-0.775	-0.303	-0.845	-0.290	-0.940	-0.278	-0.892
	(1.731)	(1.270)	(1.713)	(1.219)	(1.735)	(1.224)	(1.755)	(1.276)
Housing Price Index	0.027	0.061	0.031**	0.041	0.026*	0.028	0.026*	0.030
	(0.024)	(0.054)	(0.014)	(0.056)	(0.013)	(0.055)	(0.013)	(0.050)
Dem State					-0.000	0.004	-0.000	0.004
					(0.000)	(0.002)	(0.000)	(0.002)
Rep State			0.010	0.036	0.008	0.042	0.008	0.043
			(0.023)	(0.031)	(0.021)	(0.034)	(0.021)	(0.033)
Legal Rank			-0.025**	-0.044	-0.026**	-0.040	-0.026**	-0.041
			(0.009)	(0.026)	(0.010)	(0.027)	(0.010)	(0.028)
GSV Data Breach							-0.002	-0.004
							(0.004)	(0.006)
Year-Quarter FE	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
State FE	No	Yes	No	Yes	No	Yes	No	Yes
Observations	1,250	1,248	1,242	1,240	1,235	1,233	1,235	1,233
R-squared	0.083	0.219	0.090	0.230	0.094	0.237	0.094	0.238

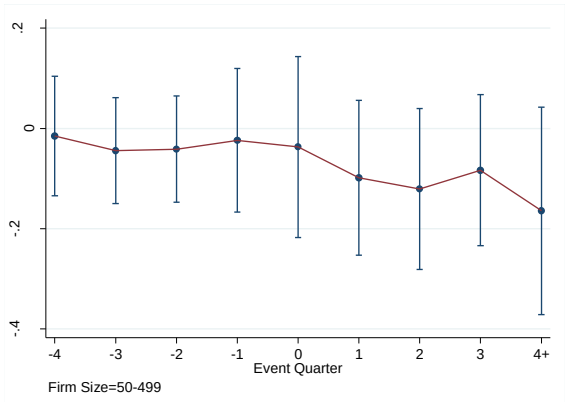
Appendix E: Evolution of employment by smaller and younger IT service firms

The figures below plot the evolution of IT employment at smaller and younger IT service firms in treatment groups relative to the control groups. The y-axis represents the coefficients on the dummy variables indicating the timing of breach notification law passage and the x-axis represents the event quarter centered around the quarter when breach notification law is signed (Event Quarter=0). The dots represent the point estimates and the vertical bars represent the 95% confidence intervals (see also table 5).









VITA

Tianjian Zhang

Candidate for the Degree of

Doctor of Philosophy

Thesis: THREE ESSAYS ON THE ECONOMICS OF CYBERSECURITY

Major Field: Business Administration with a concentration in Management Science and Information Systems

Biographical:

Education:

Completed the requirements for the Doctor of Philosophy in Management Science and Information Systems at Oklahoma State University, Stillwater, Oklahoma in May, 2020.

Completed the requirements for the Master of Science in Mathematics at Oklahoma State University, Stillwater, Oklahoma in July, 2015.

Completed the requirements for the Bachelor of Science in Mathematics at the Chinese University of Hong Kong, New Territories, Hong Kong SAR in 2010.

Experience:
Research Assistant at the Institute of Economics and Finance, Chinese University of Hong Kong, 2010-2012.

Professional Memberships:
Association of Information Systems (AIS), Institute for Operations Research and the Management Sciences (INFORMS), Production and Operations Management Society (POMS), The American Finance Association (AFA).