Cybersecurity Investments and the Cost of Capital

Taha Havakhor[*]
Temple University
taha.havakhor@temple.edu

Mohammad S. Rahman
Purdue University
mrahman@purdue.edu

Tianjian Zhang
City University of Hong Kong
ztjtjz@gmail.com

Abstract

We examine a potential path to value-creation by cybersecurity investments: a reduction in a firm's cost of capital. Building on the existing literature on corporate finance, we suggest that given the business-ending threats of cybersecurity incidents and the importance of cybersecurity investments to the future well-being of the firm, disclosing cybersecurity investments in proper channels of communication with investors (e.g., in Security and Exchange Commission, SEC, filings) likely reduces information asymmetries surrounding a firm's fundamental risks and leads to the investors' lowering the premiums charged on the borrowed capital. Empirically, we find that disclosing cybersecurity investments are associated with: a) a reduction in cost of capital (but not a reduction in operational costs, as expected in case of general IT investments), and b) a generally positive value as evidenced by robust, book-keeping measures of performance such as returns on assets and sales. Additionally, we show that both informativeness of the disclosure and the extent of the firm's analysts' coverage strengthen the cybersecurity investment and cost of capital link. Thus, this study establishes that the value of cybersecurity investments extends beyond their preventive benefits and limited market reactions and clarifies an important underlying mechanism through which cybersecurity investments create business value.

Keywords: Cybersecurity investment, cost of capital, SEC disclosure, return on assets, return on sales, information asymmetry, informativeness of disclosure, analysts' coverage

JEL Codes: D82, M41, O33

[*] The authors thank Sezgin Ayabakan, John D'Arcy, seminar participants at the City University of Hong Kong and the University of Delaware. All errors are ours.

1. Introduction

Past research on organizational cybersecurity investments has pioneered the understanding that such investments result in superior prevention from future operational disruptions (e.g., Kankanhalli et al. 2003; Kwon and Johnson 2014; Angst et al. 2017; Kwon and Johnson 2018). The value of such strategic choices, in the form of short-term market reactions (i.e., in terms of cumulative abnormal return indices) and the market valuation of current investments (i.e., in terms of Tobin's Q), are well-documented (Bose and Leung 2013; Bose and Leung 2019). However, the current findings do not consider the impact of institutional factors and players that profoundly drive the performance and survival of firms (Gao et al. 2017; Singh et al. 1986). Particularly, financial capital markets determine the cost of capital, which is a fundamental input to superior performance. This is because if the market affords a lower cost of capital for a firm, it can either invest in net-present-value-positive (NPV-positive) expenditures or leverage the overall base cost decrease to increase profit even if the revenue level remains unchanged. In other words, aside from internal investments, external investments – powered by affordable borrowed capital – can boost organizational performance, and such performance gains might be tied closely to cybersecurity investments. We are not aware of any study that examined the role of external stakeholders, who provide capital in form of both debt and equity, in assessing the impact of cybersecurity investments on firm performance.[1]

In this paper, we examine the capital market's reaction, as measured by variations in the firm's cost of capital, to cybersecurity investments of a firm. Anecdotal evidence, including Moody's recent effort to explicitly codify cyber risk in the rating of a firm (Fazzini 2018), suggests that cybersecurity concerns are profoundly impounded in the market's risk perception of the firm. Research in finance and accounting has also documented changes in the cost of capital based on investments that change the fundamental risks

[1] It is worth noting that cost of capital includes critical information that short-window market reaction measures and market valuations of firm investments do not consider. For instance, neither of the two categories of indices consider external rewards in the form of debt. Debt is a critical part of the capital structure in a firm and profoundly influences corporate investment strategies. Notably, debt is often exclusively rewarded by financial institutions, unlike equity which can also be supplied by retail investors. Thus, a firm's access to debt indicates information about an important category of institutional stakeholders that may otherwise fall in the blind spots of the usual indices of firm value examined in the literature on the business value of IT.

faced by a firm (Dhaliwal et al. 2011; Sharfman and Fernando 2008). Essentially, an improved risk perception causes the capital market to accept lower risk premiums on equity for a firm or allow it to acquire higher levels of leverage, thereby, lowering the firm's cost of capital.

This mechanism is worthy of a thorough inquiry because extrapolations from the existing literature on the business value of IT (BVIT) do not sufficiently explain the business value of cybersecurity investments and overlook cybersecurity's unique value-creating facets. Arguably, by only considering the known value-creating mechanisms through which the general IT operates, cybersecurity investments appear to have very little to contribute to firm value. Particularly, the BVIT literature has identified the increased operational efficiency and reduction in production costs (Brynjolfsson and Hitt 2003; Tambe 2014) as well as the creation of competitive advantages through creating superior digital products and services (Bharadwaj et al. 2013; Bharadwaj 2000; Keen and Williams 2013; Melville et al. 2004; Pagani 2013) as two main value-creating channels. However, neither of these known mechanisms can sufficiently explain the business value of cybersecurity investments, which have a cost-of-doing-business nature.

First, cybersecurity is not a direct input or throughput of production and does not directly contribute to reducing coordination or transaction costs. It is possible that cybersecurity investments can cut possible operational losses due to their preventive nature. However, operational losses in many cybersecurity failures are temporary (Campbell et al. 2003). As such, the business value of cybersecurity investments can hardly be explained by a reduction in production costs.

Second, the path to value creation by creating sustained advantages in competitive markets is also not sufficient to explain the business value of cybersecurity investments. General IT has demonstrably enabled transformative digital business models and contributed to tangible changes in products and services purchased by consumers. Those digital transformations, either in the form of smoothing logistics operations that facilitate quick deliveries or through more overt changes in the features of products and services, often help a firm differentiate itself from its competitors and reap competitive gains. However, the preventive impacts of cybersecurity investments are rarely tangible in the features of products and services offered to consumers, and therefore, may remain under-rewarded in product markets. Moreover, these investments rarely contribute to operational efficiencies or consumer surplus (in the form of price reduction, for instance). Hence, the gains of investment in cybersecurity and losses due to not investing in them are *not* symmetric. That is, although cybersecurity incidents are disruptive and put an impacted firm at a competitive disadvantage (Cavusoglu et al. 2004), firms taking preventive measures may not benefit from competitive gains due to the lack of market visibility to those measures.[2]

Although the two known value-creating mechanisms for general IT may not sufficiently explain the business gains from cybersecurity investments, these investments' role in mitigating an increasingly existential threat to the firm provides insights about a value-creating path that is less examined in the BVIT literature. The existing literature on corporate finance (Dhaliwal et al. 2011; Easley and O'hara 2004; Sharfman and Fernando 2008) suggests that while organizational actions dealing with outstanding risks – such as the risk of the loss of reputation and future sales – may go unnoticed or under-rewarded by consumer markets, they catch the attention of investors. In short, because investors are interested in assessing the long-term well-being of a firm, they look for, sense, and scrutinize information that pertains to the reduction of fundamental risks that a firm faces. Absent such information, i.e., under high levels of information asymmetry between the firm and its investors about major risks and measures to counter them, investors charge higher premiums for the capital they provide, resulting in an increase in the firm's *cost of capital*.

Disclosing cybersecurity investments (DCIs) can reduce the *information asymmetries* about a firm's key element of risk, i.e., the cyber risk, and subsequently, its cost of capital. On the one hand, the sharp spike in the occurrence of cybersecurity incidents, their severity, and their business-ending impacts has elevated cybersecurity risk to an outstanding risk for investors and arbitrageurs. For instance, Moody's announced in 2018 that the business-ending risks of cybersecurity have become so salient that the company will soon codify its long-standing evaluations of cyber-risk into a stand-alone cyber-risk rating, along with its credit ratings (Fazzini 2018). The move highlights the significance of cyber risks for investors as this is

[2] This is not to say that firms cannot come up with innovative solutions that give visibility to cybersecurity protections in features of their offered products, services, and markets. Rather, the point is that cybersecurity protections are *currently* rarely included in product/service packaging/presentation or reflected in offered prices.

the only technological risk currently being elaborately considered by investors, along with the traditionally-considered financial risks. On the other hand, there is robust evidence that firms with higher levels of investment in cybersecurity face significantly lower levels of cyber incident occurrence (Kwon and Johnson 2013; Kwon and Johnson 2014; Wang et al. 2013). For instance, Kwon and Johnson (2014) found that investments in cybersecurity applications reduce the hazard of future incidents by 27 percent in healthcare settings. In the sample of firms accessible to us, which spans across various industries and covers more recent years, up to 2018, firms with a DCI in a given year face a 33 percent decrease in the hazard of a cybersecurity incident happening in a subsequent year. Given both the evidence on the salience of cybersecurity risk to investors and the persistent evidence to support the effectiveness of cybersecurity investments, it is only natural to ask if there is any empirical trace that shows the impact of DCIs on the cost of capital.

Since capital is a vital value-creating input that a firm depends on, reducing the cost of accessing it can widen the profit margins (Sharfman and Fernando 2008). Nonetheless, this conceivable connection between cybersecurity investments and the reduction in cost of capital has not been empirically examined to this date. Moreover, the cost of capital is a tangible concept, well-understood by executives and financial managers (Frank and Shen 2016); examining its link with DCIs can also enhance the understanding of corporate executives of the role of cybersecurity investments in the value-creating apparatus of the firm.

To fill the aforementioned void, we start our empirical approach by constructing a sample of publicly disclosed cybersecurity investments based on public firms' SEC filings. The economic impacts of DCIs are first tested in an observational sample of 74,755 firm-year observations (belonging to 6,058 firms), spanning from 2000 to 2018. The main identification strategy in this approach includes instrumenting DCIs. To complement the strength of our causal inference, we further test our hypotheses in a quasi-experimental – difference-in-differences settings – where the selection and exogeneity issues in the design are addressed by matching (based on pre-treatment trends) and instrumenting the selection to treatment, i.e., disclosing cybersecurity investments in SEC filings for the first time.

We start by providing evidence showing that DCIs reduce a firm's costs of accessing critical capital in the form of equity and debt. Confirming the proposed mechanism through which DCIs cut a firm's cost of capital, i.e., reducing information asymmetries about a firm's future cyber risk, we show that the impact of DCIs on reducing cost of capital is greater when: a) the firm is more informative in its disclosures of cybersecurity investments, and b) more analysts cover (and interpret) the firm's actions and disclosures. Given the unfolded influence of DCIs on cost of capital, which is a key input to value creation, we trace potential impacts of DCIs on ROA and ROS as book-keeping measures of performance. We find that DCIs impact the future, but not contemporaneous, values of ROA and ROS, providing fresh evidence about value-creation through DCIs as evidenced by book-keeping indices.

This study makes a unique contribution to the literature by introducing a previously unknown mechanism through which cybersecurity, as a specific type of IT, creates business value. In doing so, it connects the literature on corporate finance to a key element of organizational digital investments that impacts the increasingly significant, cyber risks accrued to a firm. This discovery complements the existing BVIT literature, which has highlighted the role of IT investments in decreasing production costs and creating competitive advantages through digital transformations but had not yet considered a path to value through reducing fundamental risks and its consequential impact on the reduction in the frictions of accessing critical financial resources. Building on this finding that ties cybersecurity investments to a necessary source of growth, competition, and survival, the study is also the first, to the best of our knowledge, to document traces of cybersecurity impact on book-keeping measures of firm performance. Additionally, our study recognizes institutional investors who almost exclusively reward capital in the form of debt, as a key subset of stakeholders that reward a firm for its cybersecurity investments. This recognition comes to light because cost of capital includes information about both equity, which is rewarded by retail and institutional investors, and debt, which is almost exclusively rewarded by institutional investors. Finally, the study highlights the importance of managing public disclosures to include useful information about the firm's cybersecurity activities along with other traditionally-included figures and activities reported in public filings, such as those reported to the SEC.

2. Theoretical Development

2.1. Cost of capital, risk assessment, and information asymmetry

Cost of capital is fundamental to various activities a firm undertakes, including investing in growth and survival projects, and is closely tied to firm profitability (Easley and O'hara 2004). Financially constrained organizations, i.e., those with high cost of capital, reduce their strategic activities (Campello et al. 2010; Hubbard 1998) such as their investments in R&D (Hall and Lerner 2010), labor hoarding in financial crisis (Sharpe 1994), asset restructuring (Ofek 1993), and product-market competitions (Chevalier 1995). Moreover, access to capital is critical for firm survival as financing frictions can force a firm to forgo NPV-positive investment opportunities that it would otherwise capitalize on (Faulkender and Petersen 2012). These NPV-positive investments directly impact firm performance.

Under the assumption of no frictions in capital markets, the supply curve for funds should be flat, yet the *information asymmetries* between arbitrageurs and the firm (Greenwald et al. 1984; Myers and Majluf 1984) create imperfections causing the supply curve to be upward sloping (Hennessy and Whited 2007). In other words, borrowing firms are not equal in the eyes of investors in their payback and growth ability, and rather, firms are heterogeneous in terms of the investment risk they pose. In that case, investors compensate for the risks of their investment by charging a higher premium on the capital they provide.

To lower their cost of capital, firms often engage in activities that increase transparency and reduce information asymmetry (Easley and O'hara 2004). As such, high-quality accounting standards (Barth et al. 2013) and voluntary disclosure of critical firm activities (Cheynel 2013; Shroff et al. 2013) are all cited as actions aimed to reduce information frictions in capital markets. Moreover, soliciting the services of business analysts to cover activities of a firm (mostly requested by investment banks) is among other actions taken by creditors to reduce information frictions in capital markets.

Since investors base their assessment of a borrowing firm on its fundamental value, factors contributing to the borrower's significant risks of doing business are of paramount importance in shaping the investment risk that the investors perceive (Cheng et al. 2014). As such, although transparency is a necessary condition to reduce information asymmetries in capital markets, the conveyed information to investors should increase their positive evaluation of the fundamental value of the firm. For instance, (over)optimism in analysts' forecasts is shown to reduce the frictions in accessing external financing (Bradshaw et al. 2006). More importantly, investors reduce the premium they demand in exchange for capital when receiving information that reduces the perceived risks a business faces. The existing literature in strategic management (Sharfman and Fernando 2008) and corporate finance (Dhaliwal et al. 2011) is consistent in showing that firms with a reduced legal and market risks (due to following expected social, environmental, and governance norms) benefit from remarkably lower cost of capital, especially when the organizational measures in cutting those risks are disclosed by the firm (Dhaliwal et al. 2011), and externally covered by analysts (Luo et al. 2015).

Among potentially significant risks to a business are the risk of cybersecurity failures, and therefore, measures to reduce such a risk and disclosing them have the potential to influence investors' evaluation of a firm's fundamental value, and subsequently, its cost of capital. Despite this potential, whether or not investors actually consider cybersecurity risk a threat to the fundamental value of the firm remains an empirical question that is worth exploring. Moreover, whether or not cybersecurity investments can be effectively disclosed by firms and parsed by investors or their interpreting proxies (e.g., analysts) is another area where empirical evidence is still lacking.

2.2. Cyber risk and the disclosure of cybersecurity investments

Cybersecurity breaches and failures have been on the rise, plaguing businesses with disruptions beyond operational glitches. These events 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. With their extended impact on the broader operations and survival of the firm, cybersecurity breaches and failures pose a particular risk, i.e., the *cyber risk*, which can impact the fundamental value of a firm. Although there is limited academic evidence about whether or not a firm's vulnerability to cyber risk is part of the estimation of the firm's fundamental value, some pieces of anecdotal evidence can be informing. For instance, the significance of cybersecurity damage to a firm's fundamental value and the subsequent reaction by investors is exemplified in Standard and Poor's report downgrading the 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…"

This anecdote, and other similar reactions such as Moody's inclusion of cyber risk rating, reflect the issue of cyber risk being under the radar of investors. As such, it is conceivable that alerted investors may also take into account the measures to counter these incidents (especially by unimpacted firms) when evaluating the fundamental value of a firm and determining the premium it has to pay in exchange for capital.

Particularly, empirical studies on cybersecurity investments have documented their preventive value 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, it was 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 data breaches) in hospitals are associated with lower security failure rates, whereas 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 substantive cybersecurity investments in hospitals are more effective than symbolic adoptions of cybersecurity technologies in mitigating 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. As such, the preventive value of cybersecurity investments is well-documented and undisputed.

In sum, investors' observing and reacting to cybersecurity disruptions should, over time, make cyber risk a key component of evaluating the fundamental value of borrowing firms. Moreover, the overwhelming evidence supporting the preventive value of cybersecurity investments should make their voluntary disclosure – through proper channels with investors such as reports filed with the SEC in the U.S. – instrumental in reducing information asymmetries about a firm's ability to deal with the cyber risk. Subsequently, these disclosures should reduce the premium that the investors charge the firm for the capital it borrows. As such, we hypothesize that:

> **Hypothesis 1:** Disclosing cybersecurity investments (DCIs) will be associated with a lower cost of capital for a firm.

2.3. Boundary conditions

Since DCIs reduce cost of capital by reducing information asymmetries about a firm's ability to deal with the cyber risk, their impact is highly contingent on the extent to which those information asymmetries are effectively diminished. As such, both the quality of information disclosed by the firm as well as the ability of investors to parse the disclosed information are critical factors.

2.3.1. The moderating role of disclosure informativeness

The existing literature on disclosure and its impact on information asymmetry strongly emphasizes the importance of granular information availability and data quality (Botosan 1997; Chen et al. 2009; El Ghoul et al. 2011; Hail and Leuz 2006; Khurana and Raman 2004) as well as transparency (Barth et al. 2013). Notwithstanding the practical implications of its findings, the core premise of this body of research is very simple and intuitive: investors will not be able to overcome their information deficit unless the disclosures are detailed and transparent enough, or in other words, *informative*. For instance, Barth et al. (2013) discuss that higher quality in accounting standards, such as recognizing financial instruments that affect earnings, can enhance the transparency of earning statements, and show that such added informativeness is indeed paid off by a lower cost of capital.

An *a priori* judgment about the impact of informativeness in case of disclosing cybersecurity investments is less straightforward, though. On the one hand, the general principle of granularity and transparency suggests that firms disclosing more information about their cybersecurity investments allow investors to better evaluate the fundamental value of the firm. Moreover, insights from the existing literature on the preventive value of substantive cybersecurity investments relative to symbolic ones (e.g., Angst et al. 2017) also suggest that organizations should share enough details with investors to assure those investors about their dedication to the disclosed investments and show that those investments are well planned.

On the other hand, the existing literature on the motivations of external hackers and intruders suggests that sharing additional information about cybersecurity investments may attract unwanted attention from malicious actors who are ready to exploit targets that they know enough about. Specifically, 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. Firms disclosing granular information about their cybersecurity can become attractive targets for both profit- and fame-driven hackers. Disclosing information about particular investments, such as disclosing the name of a partner firm that supplies intrusion detection services, can reduce the search costs for profit-driven hackers who should otherwise actively gather clues about the cybersecurity infrastructure of the firm. Moreover, fame-driven hackers may perceive a firm's broadly disclosing information about its counter-breach initiatives as a challenge invitation. In both cases, the informativeness of disclosure may cause unintended outcomes by attracting malicious outsiders.

As such, knowledgeable investors may perceive a firm sharing detailed information about its investment as one that has carelessly opened up itself to more cyber risks. Absent any prior settling of the issue in the existing literature, the question about whether investors interpret the sharing of information as a careless act or as one that instills trust is a purely empirical one. Therefore, we frame the second set of our hypotheses as two competing ones:

> **Hypothesis 2a:** The informativeness of the disclosed cybersecurity investments *strengthens* the negative association between DCIs and cost of capital.
>
> **Hypothesis 2b:** The informativeness of the disclosed cybersecurity investments *weakens* the negative association between DCIs and cost of capital.

2.3.2. The moderating role of analysts' coverage

Analysts are experts who follow firms' strategic activities and publish opinion pieces about the firms and their stocks. In doing so, they play a critical role in gathering and interpreting information that is relevant to a firm's fundamental value (Dhaliwal et al. 2011; Easley and O'hara 2004; Irvine 2000). As experts in the industry, analysts are shown to reduce information asymmetries by operating as "information bridges" that translate signals sent from firms into insights that are comprehensible by investors and significantly contribute to returns that a firm earns (Barber et al. 2001; Luo et al. 2015; Womack 1996). For instance, Luo et al. (2015) show that analysts play a critical role in helping firms increase their returns when engaging in activities that boost their corporate social responsibility ratings.

Particularly, analysts are shown to be effective in commenting on technological initiatives that organizations undertake. For instance, existing literature (Benner 2010; Benner and Ranganathan 2012; Zuckerman 2000) shows that analysts are effective in applying institutional pressures on firms they cover to make them conform to new technological practices, especially in cases of disruptive technological changes.

That said, not all firms benefit from the same level of coverage, and so, some firms are endowed with a higher number of informational bridges that help reducing investment information asymmetries. Therefore, as more analysts follow the actions of a firm, it is more likely that clues about its cybersecurity investments are scrutinized and relayed to investors. As such, if an observed negative association between

DCIs and cost of capital is truly due to reducing information asymmetries, firms with more informational bridges (analysts' coverage) should do so more successfully. Hence, we hypothesize that:

> **Hypothesis 3:** The extent of analysts' coverage that a firm receives *strengthens* the negative association between DCIs and cost of capital.

3. Methods

3.1. Data and sample

In creating our initial sample, we followed the guidelines by Gordon et al. (2010) and obtained SEC disclosures of public firms, from 2000 to 2018. A firm was kept in the sample only if: all of the firm's financial information was available, the firm's industry classification was not missing, and the values of the other variables in our empirical estimation (discussed below) were available. Our data excludes foreign firms, including those firms that are listed in the United States as common stock or American Depositary Receipts. We further eliminated firms in banking, insurance, and real state, using Fama and French (1997) industry identifications, and winsorized the data in each 1 percent tail, following the work by Frank and Shen (2016). This process resulted in 74,755 observations of 6,058 firms active mostly in manufacturing, information, retail, wholesale trading, utilities, transportation and warehousing, and healthcare.

3.1.1. Measuring the disclosure of cybersecurity Investments

We measure a firm's cybersecurity investment disclosures by considering the *extent of emphasis* on those investments disclosed in SEC filings. We measure a firm's extent of disclosing cybersecurity investments, **DCIs,** in year t by considering the extent to which firms emphasize such investments in their SEC filings. Various Securities and Exchange Commission (SEC) reports (10-K, 10-Q, 8-K, 8-K/A) for the observations in the sample were collected from SEC's EDGAR database.[3] Paragraphs containing a set of some general keywords pertaining to cybersecurity (listed in Appendix A) were highlighted automatically, by a search engine, and the reports with at least one hit were then manually inspected by two research assistants. During this process, observations irrelevant to a cybersecurity announcement, and those

[3] The results of the study remain qualitatively unchanged when only 10-K reports are considered. These findings are discussed under the "Robustness Checks" section.

pertaining to cybersecurity but irrelevant to a cybersecurity investment (e.g., a statement pertaining to cybersecurity risks the firm faces, but not the investments it makes) were also marked. Out of 6,058 firms in the sample, 1,877 firms (almost 31 percent) had at least one report with a confirmed DCI.

Adapting the measure of IT emphasis in SEC reports from Steelman et al.'s (2019) work, DCIs 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. Steelman et al. (2019) show that lingual emphasis in SEC filings is highly correlated with the budgetary/financial emphasis on IT, and connect this emphasis measure to key indices of performance. Therefore, the intuition behind the extent measure of DCIs is that as firms assign more space in their filings to discuss their cybersecurity investments, they signal the relative increase in the importance of those investments in the limited space of reports filed with the SEC. More broadly, extant literature has used keywords to capture firm initiatives and found convergence between disclosures and actual firm initiatives (Hassan et al. 2019; Hoberg and Phillips 2010; Hoberg and Phillips 2016; Li et al. 2013).

3.1.2. Calculating the cost of capital

Following the existing literature (e.g., Sharfman and Fernando 2008; Dhaliwal et al. 2011), the main outcome variable of interest, cost of capital, is expressed as the firm's after-tax weighted average cost of capital (WACC):

$$WACC = r_E + \cdot \; r_D(1 - T),$$

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 based on data from COMPUSTAT.

3.1.3. Boundary condition moderators

To assess the **informativeness** of cybersecurity investment disclosures, we consider whether the following four major characteristics of the investments are disclosed: 1) the amount of investment, 2) the date in which the investment was made, 3) the date for which the investment becomes operationalized (or any other operational timeline offered), and 4) the name of vendor/supplier/consultant name (in case of a technological investment) or the name of startup/venture/R&D lab, where the investment is made on (in case of innovational investments)[4], are disclosed. The measure considers the number of investment characteristics disclosed divided by 4 (highest possible)[5]. In cases of multiple investments being disclosed, the average value of informativeness for each disclosed investment is considered for the extent of informativeness of disclosures in each year. Also, following the existing literature (Bhushan 1989), we operationalize **coverage** as the natural log of (1 + number of analysts covering a firm), sourcing the raw information about the number of analysts from the IBES database.

3.1.4. Controls

We control for a few firm-level variables that are frequently used (Bardhan et al. 2013; Havakhor et al. 2019; Mithas and Rust 2016; Mithas et al. 2012; Mithas et al. 2017) as time-varying covariates when estimating business profit and costs in conjunction with digital investments. In particular, **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.

In addition to these covariates, we also include the extent of firm's IT expenditure **(IT_Exp)**, since it is plausible to assume that a firm's reduction in cost of capital can simply be due to an increase in its overall

[4] We consider cybersecurity investments in internal R&D or external venture capital investments in cybersecurity startups or acquiring them as innovational investments.

[5] We acknowledge that the four dimensions may carry different weights.

IT expenditure, which at the same time triggers investments in cybersecurity. Therefore, we include this important control variable to avoid the identification issue due to omitting IT_Exp from the model. We estimate the overall IT expenditure by measuring IT stock from the Computer Intelligence (CI) database (Chwelos et al. 2010).

Since several general, non-cybersecurity factors can determine a firm's cost of capital, it is imperative to ensure the effect of those factors, especially if time-varying, is reasonably accounted for in our estimation of cost of capital. Therefore, we include several additional controls that the literature (e.g., Sharfman and Fernando 2008; Luo et al. 2012) has identified as key factors influencing the cost of capital. We include **forecast error**, estimated as the absolute difference between the latest analysts' median consensus forecasts before the earnings announcement and the firm's actual earnings per share divided by stock prices (Barth et al. 2001), which has been shown to increase analysts' positive recommendation. Further, we include **analysts' exposure** (firm-specific experience (ln(1+number of years covering the firm) following Chen and Matsumoto (2006)), which enhances the quality of analysts as information bridges. Both forecast error and analysts' exposure adjust for the possible biases in analyst coverage a firm receives.

We also include disclosure of corporate social responsibility actions (**CSR disclosure**; the number of public disclosures about their firm's socially responsible activities in CSR newswire and Corporateregister.com), since it is known to reduce cost of capital (Dhaliwal et al. 2011). The inclusion of this variable is important because an alternative explanation for the impact of DCIs on cost of capital can be that a firm may have engaged in several activities to lower its risks, and without including those other major risk-reducing activities, the impact of cybersecurity investments cannot be identified. For a similar reason, we control for the extent of **non-cyber disclosure**s (Ln(# of non-cyber sentences in the SEC reports), following Li 2008) as another indicator of the disclosure of other activities related to the social risk a firm faces.

Finally, to better identify the impact of DCIs' informativeness, it is important to partial out the impact of the general informativeness that a firm shows in its SEC filings. To do so, we control for a general measure of informativeness in SEC reports (**SEC informativeness**; Ln(# of the number of informative numbers while dropping dates and section identifiers, etc.) in SEC reports (Dyer et al. 2017)).

The measures and data sources for each variable are summarized in Table 1. Table 2 Panel A presents the correlation matrix, and Panel B presents descriptive statistics for the key variables. Specifically, the last column in Panel B reports the t-statistics comparing the means for firms with DCI always equal to zero (4,181 firms) and firms that have at least one observation with DCI greater than zero (1,877 firms). First, the two types of firms are different in their average WACC, with firms showing at least one DCI disclosed having a lower WACC. These comparisons also reveal that firms with no DCI have a slightly larger asset size, but show moderately lower amounts of IT and R&D expenditures. More importantly, both groups show insignificant differences in terms of known, general contributors to the cost of capital, namely, forecast error, analysts' exposure, CSR disclosure, non-cyber disclosure, and SEC informativeness. This implies that the significant difference in WACC between the two groups may not be explained sufficiently by known, general factors contributing to WACC. This provides some model-free evidence pertaining to the importance of considering DCIs in explaining cross-firm differences in terms of WACC.

--- Insert Tables 1 and 2 about here ---

3.2 Estimation

Our main empirical estimation starts with the following equation:

$$(EQ.1)\ \ Outcome_{it} = \beta \cdot DCIs_{it} + \gamma \cdot control_{it} + Industry\_YEAR + c_i + \epsilon_{it}$$

where subscripts i and t denote firm i in year t. ϵ_{it} is the error term, DCIs is the extent of disclosing cybersecurity investments, control is a matrix of control variables outlined above, c_i is the firm fixed-effect, and Industry_YEAR represents the industry-year fixed-effect dummies. To test the boundary conditions of our theory (H2 and H3), we add informativeness of disclosures (*Informativeness*) and the extent of analysts' coverage (*Coverage*) and their interaction with DCIs to estimate the following equation:

$$\begin{aligned}(EQ.2)\ Outcome_{it} = {} & \beta \cdot DCIs_{it} + \lambda \cdot Informativeness_{it} + \xi \cdot Coverage_{it} \\ & + \eta \cdot Informativeness_{it} \times DCIs_{it} + \phi \cdot Coverage_{it} \times DCIs_{it} \\ & + \gamma \cdot control_{it} + Industry\_YEAR + c_i + \epsilon_{it}\end{aligned}$$

In our estimations, we treat DCIs as endogenous, since some unobserved time-variant factors may simultaneously influence both this variable and the error term. Therefore, this variable and its product terms are instrumented using a panel two-stage least squares (2SLS) procedure.

To identify a set of appropriate instruments (X_{it}) to exogenously predict DCIs in a 2SLS procedure, we include a set of Hausman-type industry averages, following the existing literature (Aral et al. 2017; Cachon et al. 2018; Lu et al. 2017; Mithas and Rust 2016). Specifically, we consider the industry averages of cybersecurity breaches (**Ind_Breach**[6]), measured as the average number of cybersecurity breaches (reported in the Privacy Rights Clearinghouse website (www.privacyrights.org)) faced by the firms in the industry for the past five years, as a relevant instrument since it can influence the firm's perception of its cybersecurity threat and consequently impact its DCIs. Moreover, we consider the industry average of DCIs (**Ind_DCI**[7]), since the institutional theory of the firm suggests that firms engage in activities similar to their peers to gain legitimacy (DiMaggio and Powell 1983). Specifically, given the importance of cybersecurity threats, firms are incentivized to keep up with the cybersecurity investment disclosure norms in their industry.

Finally, we use a proprietary dataset of 70 million online resumes supplemented by a major online job search platform to measure the average number (ln(1+#)) of cybersecurity talent (**Ind_Talent**[8]) recruited in the firms in the same industry. This number can influence DCIs as it proxies the supply size of talent available to a firm if it intends to invest in cybersecurity. Given cybersecurity investments require the support of human capital to succeed, the availability of expert workforce in the industry can positively influence a firm's inclination to invest in cybersecurity, and subsequently, influence the disclosure of such investments. The cybersecurity talent in a firm for a given year 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

[6] Mean=2.84, SD=3.21, Median=2.61, Min=0, Max=13.

[7] Mean=0.28, SD=0.18, Median=0.33, Min=0, Max=0.43.

[8] Mean=7.25, SD=6.76, Median=7.65, Min=5.36, Max=9.08.

in cybersecurity-related projects/positions before recruitment. Cybersecurity talent on the industry-level is then aggregated from the firm-level measure.[9]

While Ind_Breach, Ind_DCIs, and Ind_Talent have theoretical relevance to DCIs, as discussed, it is unlikely that time-varying factors specific to a firm and omitted from our specification drives the level of the instruments given their industry-wide nature. Further, the exclusion of the instruments from the second stage of our 2SLS specification does not bias the estimates since these industry averages either influence a firm's cost of capital through its DCIs or create an industry-level effect[10], which is removed by the inclusion of industry-year dummies in our models. Therefore, the exclusion restrictions are met for the set of our instruments.

The set of these instruments show strong statistical relevance to the endogenous variables as shown in stage one estimations presented in Appendix C. Specifically, the Cragg-Donald Wald F Statistic exceeds 5% maximal bias of the IV estimator relative to OLS in both equations (Stock and Yogo 2005), rejecting the null hypothesis of the equations being weakly identified (For Equation (1): F-statistic = 122.73, Stock and Yogo's critical value for 1 endogenous variable and 3 instruments= 13,91; For Equation (2): F-statistic = 88.92, Stock and Yogo's critical value for 3 endogenous variables and 9 instruments is 16.10). 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): $p = 0.317$; For Equation (2): $p = 0.211$).

4. Results

4.1. Main findings

We conduct our analysis by providing estimations of EQ.1 using both a regular fixed-effects estimation and a panel 2SLS fixed effects regression (columns 1 and 2 in Table 3). We conduct these analyses to present the potential upward bias that may occur if an instrumented measure of DCIs is not used to conduct

[9] Appendix B provides further details about this measure.

[10] For instance, investors may generally lower the cost of capital for firms in industries with low Ind_Breach, but such impact is absorbed by the industry-year dummies included in the model.

our main analyses. The coefficients of DCIs in both estimations are negative and significant, consistent with H1, providing evidence that DCIs reduce cost of capital. The effect size of DCIs in the instrumented estimation (Column 2) is smaller than its effect size in the un-instrumented estimation (Column 1), suggesting that not instrumenting DCIs can present some upward bias in our estimates, hence, we present the rest of our estimations where DCIs is instrumented in the fixed effects specification. The effect size from Column 2 suggests that an otherwise-average firm with a DCIs value that is one standard deviation above the mean in the sample has access to capital at a rate that is 13 percent lower compared to what its counterparts have access to. Column 4 in Table 3 presents the estimation of EQ.2 with both coverage×DCIs and informativeness×DCIs coefficients being negative and significant (at $p < 0.1$ and $p < 0.05$ levels). These findings support H2a and H3, providing evidence that the impact of DCIs on cost of capital is contingent upon how granular the information communicated in DCIs is and how well-bridged a firm is to its investors for them to sense signals sent through DCIs.

---Insert Table 3 here---

4.2. Robustness Checks

4.2.1 Alternative measures of DCI

To ensure that our initial findings are robust to variations in the measurement of key constructs, we estimated several alternative models. Table 4 presents the results of these robustness tests. First, we replaced our measure of DCIs with a binary variable that assigns the value of 1 to firms that disclose at least one cybersecurity investment in their SEC filings in that year and becomes 0, otherwise. While the measurement of the extent of emphasizing investments (the main measure of DCIs) allows us to understand how small hints versus elaborate disclosures affect a firm's cost of capital, the binary measurement allows for a sharp comparison between firms that do not engage in disclosing their investments versus the ones that do. Column 1 in Table 4 presents the results of estimating a model with a binary measure of DCIs and shows a negative and significant impact on cost of capital. Specifically, at the average levels of coverage and informativeness, an otherwise-average firm with at least one public disclosure of a cybersecurity investment has access to capital at a rate that is 11 percent lower compared to what its counterparts with no disclosure have access to.

The other alternative (Column 2) estimation uses a measure of DCIs where only 10-K reports are scrutinized. We follow this estimation because other types of SEC filings (e.g., 10-Q) analyzed in the original model are periodic; hence, the annual report filing (10-K) might include some double- or multiple-emphasizing of the same investment.

Moreover, the third estimation (Column 3) uses the ratio of cybersecurity-related press releases in year t to all press releases in year t by firm i, i.e., press release emphasis, as an alternative measure of DCIs. While the SEC filings are valid sources of disclosing a firm's cybersecurity investments, press releases are other important means of relaying important information about the firm to the stakeholder. Therefore, we re-evaluated our model, using this alternative measure of DCIs to ensure that our findings are not due to other unmeasured aspects of the firm's operations that are also mentioned in SEC filings and covary with the portions emphasizing cybersecurity. It is, nevertheless, unlikely that those covarying aspects are also present in press releases that have a targeted message (about the cybersecurity investment). The results of both Column 2 and 3 qualitatively converge with the findings of our original estimation of EQ.2.

4.2.2 Alternative measures of the cost of capital

In another set of tests, we examine alternatives of the outcome variable. First, since WACC consists of costs of equity and debt combined, we run separate models with each component being the outcome variables in those models. Column 4 of Table 4 presents the results when cost of debt is the outcome variable, and Column 5 presents an estimation where only cost of equity is considered as the outcome variable. In both models, the results qualitatively converge with the original estimation of EQ.2, although DCIs show a stronger association with cost of equity (-0.135) relative to their association with cost of debt (-0.075). Given equity holders have a greater interest in the subsequent success of the firm and are also more profoundly impacted by its failures, and given cybersecurity investments are made to reduce the risk of future failures, the stronger impact of DCIs on cost of equity better showcases that the rewards in the form of a reduced cost of capital are tied closely to the attenuated risks as perceived by investors. Also, while our original measure of WACC uses a simple CAPM to estimate the expected return from holding to the firm's equity, we also test a model that uses a Fama-French 3-factor model (1997),[11] following Frank and Shen (2016), to estimate the expected equity returns (r_E). Column 6 in Table 4 presents the results of the estimation with this alternative measure of WACC and shows consistent findings with those presented in Table 3.

4.2.3. An alternative measure of analyst coverage

Our final robustness test focuses on an alternative measure of the coverage that firms receive. In our main analyses, we rely on a standard measure of analysts' coverage which considers the number of all analysts covering a firm's activities. While coverage by more analysts provides more informational bridges to parse a firm's cybersecurity investments for investors, not all analysts may scrutinize and analyze activities related to cybersecurity. It is conceivable that analysts with more exposure to cybersecurity incidents may have a heightened sense and perceive cybersecurity as a higher risk to a firm, and therefore, further scrutinize cybersecurity investments a firm makes. So, Column 7 in Table 4 considers an alternative measure of coverage, where we consider the natural log of 1 + the number of cybersecurity incidents analysts covering a firm have covered in years prior to year (t).[12] This model's estimates converge with our original findings, with the effect size of coverage×DCI being larger (and statistically more significant) than our original estimate (-0.086 at $p < 0.01$ compared to -0.034 at $p < 0.10$), indicating that this fine-tuned measure of coverage better captures the informational role of experienced analysts. Since experienced analysts have first-hand experiences about cybersecurity incidents and the business-failure threat they pose, these results also converge with our core argument that the reduction in cost of capital is, at least in part, due to the perceived threat of cybersecurity incidents and the preventive role of cybersecurity investments.

---Insert Table 4 here---

[11] The Fama-French's 3-factor model extends CAPM by adding size and value premium to account for size risk and value risk factors, which CAPM overlooks.

[12] Using Privacy Rights Clearinghouse website (www.privacyrights.org) we add up the number of cybersecurity incidents happening to all firms that analysts have covered up to year t.

4.3. Falsification tests

Our theory is built on a core premise that: DCIs regulate cost of capital due to their effectiveness in containing the risks of business failure due to cybersecurity incidents, and do so when they are communicated clearly and through enough information bridges. An alternative narrative, however, may be posed that a mere disclosure about cybersecurity, even if it is only made to clarify the risks a firm faces, can also reduce information asymmetries for investors and, therefore, be met with discounted rates for capital. To understand if this counter-argument can explain our findings, we conduct a falsification test replacing DCIs with a measure of disclosing cybersecurity risks **(DCRs)**. Cybersecurity risk disclosures are sections of SEC reports where a firm discloses the cyber risks it faces without explaining tangible measures taken to attenuate the risks. The measure of DCRs is created in the same fashion as DCIs except that the only paragraphs concerning disclosure of cyber risk, without the mention of a tangible cybersecurity investment, are considered in the numerator of the ratio. If the said alternative narrative explains our findings, we should find converging results in a model that replaces DCIs with DCRs. Column 1 in Table 5 reports the estimates of such a model. Notably, the coefficients of DCRs, Coverage × DCRs, and Informativeness×DCRs are all statistically insignificant. This falsification test provides empirical evidence that mere disclosure of risks without explaining tangible measures to counter them does not translate into a reduction in the cost of capital.

Further, it is imperative to rule out other outstanding sources of the cost that can also be cut due to DCIs. Otherwise, it may not be clear if the observed impacts on the reduction of cost of capital are due to the investors' re-evaluation of the broader risks (e.g., the cyber 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 (**COGS) -** all expenses directly allocated by the company to production, such as material, labor, and overhead/sales.

Column 2 in Table 5 presents the estimation of a model with COGS as the outcome variable. The results show that DCIs do not have a significant association with COGS. Also notable is the significant negative impact of the IT_Exp on COGS, which is consistent with the existing BVIT literature (Aral and Weill 2007;

Mitra and Chaya 1996; Santhanam and Hartono 2003; Zhu 2004). This, coupled with the IT_Exp's borderline significant (only at $p < 0.05$) impact on cost of capital in estimating EQ.2, further contrasts the nature of costs cut by general IT versus those cut by cybersecurity investments. As such, the findings suggest that unlike general IT, which contributes to reducing operational costs, cybersecurity investments are almost unrelated to operational efficiency, and rather, impact costs that are tied to fundamental risks a firm faces.

---Insert Table 5 here---

4.4. Further identification improvements

While our main identification strategy focuses on instrumenting DCIs and controlling for firm fixed-effects, it is possible that a firm's extent of coverage is not econometrically exogenous. For instance, a firm's heightened levels of reduced cost of capital may encourage investors to seek more scrutiny, inviting more analysts to cover the actions of the firm. Such endogeneity of coverage in our model, in turn, may bias our estimates. To see if such concerns impact our findings, we utilize a set of exogenous shocks, identified by Derrien and Kecskes (2013), and use broker closures and broker mergers as instruments that can influence the levels of analysts' coverage exogenously (Derrien and Kecskés 2013). We follow Derrien and Kecskes' approach in identifying broker closures and broker mergers through examining press releases related to the brokers in Lexi-Nexis/Factiva as well as through examining Yearbooks released by Securities Industry Association. Then, each broker's portfolio of firm coverage is identified through records in the IBES database. We use these two external shocks, closure or merger of a firm's brokers, as instruments that *reduce* the extent of coverage a firm might receive. Closure/merger is set at 1 in the event year and is 0 in the year before or after the closure/merger. We add these two instruments to the set of our Hausman-type industry-average instruments. Column 1 in Table 6 reports the estimation with this set of instruments added to the mix. While DCIs' coefficient stays significant and negative (-0.108, $p < 0.001$), the coefficient of Coverage×DCIs grows larger in effect (-0.075 compared to 0.034) and becomes significant at $p < 0.001$.

Moreover, in our original instrumental approach, we assumed that the impact of Ind_Breach, Ind_DCI and Ind_Talent is either absorbed by the inclusion of DCIs or the Industry_Year dummy. To further ensure the exclusion restrictions are met, we also ran a model with the firm-level extents of Breach and cyber Talent included as covariates in the model. This inclusion ensures that the effect of the full set of industry-level Hausman type instruments is either absorbed by their firm-level covariates (i.e., Breach, DCIs, Talent) or through the inclusion of Industry_Year dummies. Column 2 in Table 6 reports the estimation with the set of covariates added and shows that our results remain unchanged, qualitatively, under this alternative specification.

Finally, a critical unobserved factor in our model is the actual presence of cybersecurity technologies in a firm. While the information about these actual technologies is not available to us for the full period of the study, we utilized a new section of the CI database, which is available from 2010 onwards, to control for the impact of the presence of 14 types of cybersecurity-related software and technologies.[13] Specifically, we controlled for the presence of Anti-Virus Software, Network Firewall, Access Management or Identity Management Software, Network Management Software, Asset Management Software, Primary Virtual Private Network (VPN) Provider, Security Information & Event Management Software, Archiving and Backup, Network Management, Disaster Recovery Software, Surveillance Security System, Infrastructure as a Service, Storage Management or Backup and Recovery Software, Cloud Computing, as reported in the CI database. Since the installation of these software elements is reported at surveyed business units (BUs) in a firm, we use the ratio of BUs reporting an installation to the number of all BUs surveyed in that year as the value of each of the fourteen mentioned cybersecurity-related software. Column 3 in Table 6 reports the estimation of EQ.2 when these fourteen covariates are included in the model. The coefficients of DCIs and interaction terms remain qualitatively unchanged, indicating that even in observations where we can partial out the impact of actual investments, public disclosures and informational advantages play a significant role in bringing down the cost of capital.

---Insert Table 6 here---

[13] The categorization of these software and technology elements as cybersecurity-related is directly obtained from the Installation tables in the CI database.

4.4.1. A quasi-experimental approach and a difference-in-differences design

In a perfect experimental design, which is arguably either impossible in the field or too costly in corporate research, one expects to randomly assign firms to disclosure and non-disclosure groups, measure the cost of capital before and after introducing the treatment to the treatment group and measure the difference in differences between before and after the treatment measures of the cost of capital. Aside from the problems with random assignment of the treatment (which is addressed by instrumenting DCIs), our observational approach includes two types of treatment observations: a) observations where the firm becomes treated after being untreated in the prior year (an untreated$_{t-1}$-treated$_t$ firm), and b) observations that become untreated after receiving treatment in the last year (a treated$_{t-1}$-untreated$_t$ firm). Although this cross-sectional variation is informative about the average impact of treatment both in cases where treatment is introduced as well as in cases where treatment is taken away, the mix of these two scenarios introduces yet another layer of contamination to a clean and simple experimental setting. [14]

An alternative operationalization of DCIs as binary 0/1 variables allows us to compare the impact of being treated (at some point) to being untreated in the sample. Moreover, a stricter rule in retaining only untreated$_{t-1}$-treated$_t$ pairs of observation for the treatment group allows us to focus solely on the impact of *introducing* DCIs to a firm, all else being equal. In such a design, we can re-write EQ.1 as:

$$EQ.3\ \ Outcome_{it} = \beta \cdot Treat_i \times Post_{it} + \gamma \cdot Post_{it} + Control_{it} + FIRM_i + YEAR_t + \epsilon_{it}$$

Where EQ.3 would be a classic quasi-experimental design with a difference-in-differences specification. $Treat_i$ is one for firm i if the firm is treated at some point in the sample period and $Post_{it}$ is equal to 1 for the treated firms in the year that they disclose cybersecurity investments for the first time, and becomes 1 also for the untreated firms that are a direct match to a treatment pair, in the same year that the treatment firms become treated (i.e., counterfactuals before and after observations are picked

[14] One possible contamination is that investors may still consider a treated$_{t-1}$-untreated$_t$ firm in year t as one with equally sufficient cybersecurity safeguard around it due to the prior year investments, whereas an untreated$_{t-1}$-treated$_t$ firm in year t is certainly regarded as a firm in the "better-off" category. Without proper econometric adjustments, a cross-sectional approach treats the two differences as equivalent.

symmetrically around the same years as the treatment group before and after observations). In the equation above, $Treat_i \times Post_{it}$ provides the difference-in-differences (DID) estimation.

A classic DID estimation, such as the one above, results in unbiased estimates for the average treatment effect when two conditions are satisfied: a) the treated and counterfactual observations follow similar pre-treatment trends for the outcome variable (parallel trends assumption), and b) the assignment to the treatment group is reasonably random (i.e., the DID term is reasonably exogenous). However, in corporate policy choice contexts, such as selecting openness in disclosures, organizational choices are hardly exogeneous and previous trends in critical outcome variables, such as cost of capital, most likely are a factor in the self-selection in the treatment group.

The existing literature on DID designs suggests two remedies to account for the self-selection issue discussed above. First, a symmetric-date matching between the treated and untreated firms based on the pre-treatment values of outcome variables is recommended, especially when enough pre-treatment observations (at least 3 pre-treatment observations of the outcome variable) are accessible (Chabé-Ferret 2015). Although Chabe-Ferret's (2015) simulations show that matching based on covariates, instead of matching based on pre-treatment values of the outcome variable, produce considerably more biased estimates, our results remain qualitatively unchanged when we follow a covariate matching (with matching criteria being financial leverage, liquidity, cash dividend, institutional ownership, and industry (2-digit SIC)).

Second, we instrument the term pertaining to selection into treatment, i.e., $Treat_i \times Post_{it}$, with a similar set of instruments used in our observational approach to predict an exogenous estimate of $Treat_i \times Post_{it}$[15]. However, since $Treat_i \times Post_{it}$ is a binary variable, a 2SLS estimation results in biased estimates, causing a problem that is sometimes referred to as the *forbidden regression* (Wooldridge 2010). An alternative is offered by Heckman (1979) to use a control function approach, instead of 2SLS, which uses the same set of exclusion restrictions along with other controls to predict the $Treat_i \times Post_{it}$

[15] $Treat_i$ itself is a time-invariant term and therefore is absorbed by the fixed-effects while estimating EQ.3. Therefore, it does not require any instrumentation.

in a probit model, and then, includes the *Inverse Mills Ratio (IMR),* estimated from the first stage, as the control for the hazard of selection in the second stage equation (i.e., EQ.3) (Heckman 1979). We follow both matching and Heckman's procedure to correct for possible violations of the parallel trends assumption and the exogeneity of being treated.

To empirically estimate the coefficients of our DID equation, we start by identifying firm-year observations where the firm becomes first treated in the span of 2000 to 2018 (i.e., discloses a cybersecurity investment in its SEC filings). We also retain the firm-year observation in the previous year where the firm is still untreated (this provides the pre-treatment observation). Then, for each retained treated observation pair (pre and post), we try to find a match in our sample based on the past pre-treatment values of cost of capital. For instance, if we find a firm that becomes treated in 2012 for the first time, we retain the observation belonging to the same firm in 2011, and then, try to find a match (through a coarsened exact matching procedure, CEM) that has similar values of change in costs of capital in years 2011, 2010, and 2009. Once and if a match is found, the 2011 and 2012 observations of the matched counterfactual are retained in the sample (this ensures a matching symmetrically around the treatment date, per Chabe-Ferret (2015)). Given the natural variation in a sample of competing firms, finding a match based on pre-treatment values is a rare occurrence. Out of 1,877 firms that become treated at some point in our sample, we could only find a proper match for 174 of them. Therefore, our DID sample includes pre- and post- observations for those treated firms along with the same-year observations for their matched counterfactuals, resulting in 696 firm-year observations that belong to 348 firms.

Column 1 in Table 7 presents the results of estimating EQ.3. The DID estimate is -0.087 ($p < 0.001$), supporting H1.[16] This estimate suggests that for two otherwise similar firms with an average cost of capital, the one that discloses a cybersecurity investment enjoys an almost 10% reduction in its cost of capital rate in a subsequent year. Additionally, we estimated EQ.3 by replacing our treatment with a placebo that

[16] Appendix D presents the results of a relative time estimation that confirms the assumption of parallel trends, with all pre-treatment terms being insignificant and post treatment impacts showing significance consistent with EQ.3 estimations.

indicates a firm discussing cybersecurity risks in its SEC filings for the first time, without pointing to a tangible cybersecurity investment (e.g., by only discussing the cybersecurity risks that the firm faces; analogous to our DCRs measure earlier). Column 2 in Table 7 shows the results of this estimation. The placebo impact is -0.009 but not statistically significant ($p > 0.10$), indicating that a general disclosure about cybersecurity does not effectively lower cost of capital for the firm.[17]

---Insert Table 7 here---

4.5. Additional analysis: Impact of DCIs on book-keeping measures of performance

Given our initial analyses support the impact of DCIs on reducing a firm's cost of capital, we become interested to see if the impacts of DCIs can be also traced in book-keeping indices such as return on assets (ROA) and return on sales (ROS). That is, if a firm benefiting from lowered premiums capitalizes on the opportunity to borrow, the firm must see a tangible rise in its bottom-line performance because firms can turn the borrowed capital into NPV-positive investments. This expectation is a rather new proposition, as most of the existing studies on the business value of cybersecurity investments have taken an event-study approach, where returns are estimated in short windows (Bose and Leung 2013; Chai et al. 2011) or estimated in terms of stock market reactions such as Tobin's Q (Bose and Leung 2019) or 12-month stock returns (Gordon et al. 2010).

Although stock market sentiments can be reliable indicators of improved performance as measured by book-keeping indices of measures in some instances, they can also be susceptible to short-term sentiments and overreactions, especially around events that attract public reaction and popular media coverage (Alti and Tetlock 2014; Malmendier and Tate 2009; Tetlock 2007). With cybersecurity increasingly being a topic of interest by the public and the media, it is not clear how likely it is that those stock market reactions to cybersecurity investments are reliably congruent with actual changes in book-keeping indices of performance. Given the empirical importance of this question, we test this proposition in our next analysis.

[17] A difference in DID (DIDID) estimate shows that the coefficients of $Treat_i \times Post_{it} \times Coverage_{it}$ and $Treat_i \times Post_{it} \times Informativeness_{it}$, are both negative and statistically significant, supporting H2a and H3 in the quasi-experimental settings. The results of this analysis are excluded for brevity but are available upon request

Specifically, **ROA** and **ROS** are measured by net income/net sales and operating income/net sales, respectively. We also test a model with Tobin's Q as previously examined forward-looking measure of performance in the context of cybersecurity investments (Bharadwaj et al. 1999). Following Chung and Pruitt (1994), **Tobin's $\boldsymbol{Q}$** is calculated as $q\ =$ (Market value of equity + book value of inventories + liquidating value of preferred stock + long-term debt + net short-term debt)/Total assets.

Table 8 presents the estimation of EQ.1, starting with a baseline model that considers the impact on Tobin's Q, and proceeding with ROA and ROS as outcome variables. The baseline model (Column 1) shows a significant and positive impact by DCIs on Tobin's Q, showing that we can replicate the sentiment-based rewards to DCIs. More importantly, Columns 2-4 and Columns 5-7 in Table 8 present the results with the contemporaneous (t), one-lead ($t+1$), and two-lead ($t+2$) values of ROA and ROS being the outcome variable, respectively. The contemporaneous and one-lead value models do not show a significant impact by DCIs. However, the model with two-lead values shows a positive impact by DCIs on both ROA and ROS. This finding is congruent with the time-taking nature of the process through which a firm leverages its acquired capital in various growth investments. These findings show that the bottom-line impacts of DCIs extend beyond the forward-looking, sentiment-based measures of performance and can be traced in book-keeping indices, such as ROA and ROS. In sum, this evidence suggests that firms with higher levels of DCIs will most likely leverage their discounted access to capital to build business advantages and higher returns.

--- Insert Table 8 about here ---

5. Discussion and conclusions

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 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 are also met with a reduction in information asymmetry between the firm and arbitrageurs, and subsequently, cheaper access to financial resources. The collection of our findings paints a picture of cybersecurity investments that: a) connects them to the book-keeping indices of sustained performance, and b) 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 extends the work on the business value of cybersecurity investments (e.g., Gordon et al. 2010; Bose and Leung 2019) by theoretically discussing and empirically unfolding an important mechanism that can explains how the preventive value of cybersecurity turns into business value. To the best of our knowledge, this study is the first empirical work that unfolds the impact of cybersecurity investments, when disclosed publicly, on the robust, book-keeping indices of performance. Moreover, and building on the corporate finance literature, which positions investors and arbitrageurs in central roles both in assessing the firm's fundamental risks and in regulating the costs of its access to capital, we highlight the important role of engaging in cybersecurity investments in reducing frictions in financial capital markets. Our study complements the existing literature on BVIT that has highlighted a reduction in production cost and creating differentiating features in competitive markets as two main ways in which general IT contributes to value-creation and offers a third path. Recognizing the distinct facets of cybersecurity in reducing risks of business failure and having a primary cost-of-doing-business nature, we show that IT investments can pave the way for value-creation by also operating as signals of lowered risk in capital markets.

For practitioners, the finding pertaining to the impact of DCIs 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.

Moreover, a focus on cost of capital allows financial managers to better think of what they can do with the benefits they are likely to receive from engaging in and broadcasting cybersecurity investments. Particularly, while both cash flow and Tobin’s Q have long been shown, at least theoretically, to influence corporate investments (e.g., Hayashi 1982; Fazzari et al. 1988), recent evidence (Frank and Shen 2016) suggests that cost of capital contains information relevant to corporate investments that is not impounded in Tobin’s Q, which is a variable of interest most commonly used in the BVIT literature. Aside from the unique impact of cost of capital on a firm’s future investments, surveys by the Association for Financial Professional (AFP 2011) suggest that most financial managers and practitioners do not think about investments in terms of Tobin’s Q (Frank and Shen 2016) and are instead taught to think of their future investments while considering their firm’s cash flow and cost of capital. As such, crystalizing the impacts of cybersecurity investments by connecting them to a factor well-understood and leveraged by practitioners can better fuse the inclinations of IT managers, who seek to protect their firm, with those of financial managers, who actively look to find promising investment opportunities.

Further, since the market profitability of cybersecurity investments can also be traced in later values of traditional accounting indices, managers should allow enough time to 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.

References

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.

AFP, A. f. F. P. 2011. "Current Trends in Estimating and Applying the Cost of Capital: Report of Survey Results," Author Bethesda, MD.

Alti, A., and Tetlock, P. C. 2014. "Biased Beliefs, Asset Prices, and Investment: A Structural Approach," *The Journal of Finance* (69:1), pp. 325-361.

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

Aral, S., and Weill, P. 2007. "It Assets, Organizational Capabilities, and Firm Performance: How Resource Allocations and Organizational Differences Explain Performance Variation," *Organization Science* (18:5), pp. 763-780.

Bai, X., Padman, R., and Airoldi, E. 2004. "Sentiment Extraction from Unstructured Text Using Tabu Search-Enhanced Markov Blanket," *Workshop on Mining the Semantic Web, at the 10th ACM SIGKDD Conference, Seattle, WA*.

Barber, B., Lehavy, R., McNichols, M., and Trueman, B. 2001. "Can Investors Profit from the Prophets? Security Analyst Recommendations and Stock Returns," *The Journal of Finance* (56:2), pp. 531-563.

Bardhan, I., Krishnan, V., and Lin, S. 2013. "Research Note—Business Value of Information Technology: Testing the Interaction Effect of It and R&D on Tobin's Q," *Information Systems Research* (24:4), pp. 1147-1161.

Barth, M. E., Beaver, W. H., and Landsman, W. R. 2001. "The Relevance of the Value Relevance Literature for Financial Accounting Standard Setting: Another View," *Journal of Accounting and Economics* (31:1-3), pp. 77-104.

Barth, M. E., Konchitchki, Y., and Landsman, W. R. 2013. "Cost of Capital and Earnings Transparency," *Journal of Accounting and Economics* (55:2-3), pp. 206-224.

Benner, M. J. 2010. "Securities Analysts and Incumbent Response to Radical Technological Change: Evidence from Digital Photography and Internet Telephony," *Organization Science* (21:1), pp. 42-62.

Benner, M. J., and Ranganathan, R. 2012. "Offsetting Illegitimacy? How Pressures from Securities Analysts Influence Incumbents in the Face of New Technologies," *Academy of Management Journal* (55:1), pp. 213-233.

Bharadwaj, A., El Sawy, O. A., Pavlou, P. A., and Venkatraman, N. 2013. "Digital Business Strategy: Toward a Next Generation of Insights," *MIS Quarterly* (37:2), pp. 471-482.

Bharadwaj, A. S. 2000. "A Resource-Based Perspective on Information Technology Capability and Firm Performance: An Empirical Investigation," *MIS Quarterly* (24:1), pp. 169-196.

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.

Bhushan, R. 1989. "Firm Characteristics and Analyst Following," *Journal of accounting and economics* (11:2-3), pp. 255-274.

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.

Botosan, C. A. 1997. "Disclosure Level and the Cost of Equity Capital," *The Accounting Review* (72:3), p. 323.

Bradshaw, M. T., Richardson, S. A., and Sloan, R. G. 2006. "The Relation between Corporate Financing Activities, Analysts’ Forecasts and Stock Returns," *Journal of Accounting and Economics* (42:1-2), pp. 53-85.

Brynjolfsson, E., and Hitt, L. M. 2003. "Computing Productivity: Firm-Level Evidence," *Review of economics and statistics* (85:4), pp. 793-808.

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.

Campello, M., Graham, J. R., and Harvey, C. R. 2010. "The Real Effects of Financial Constraints: Evidence from a Financial Crisis," *Journal of Financial Economics* (97:3), pp. 470-487.

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.

Chabé-Ferret, S. 2015. "Analysis of the Bias of Matching and Difference-in-Difference under Alternative Earnings and Selection Processes," *Journal of Econometrics* (185:1), pp. 110-123.

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.

Chen, K. C., Chen, Z., and Wei, K. J. 2009. "Legal Protection of Investors, Corporate Governance, and the Cost of Equity Capital," *Journal of Corporate Finance* (15:3), pp. 273-289.

Cheng, B., Ioannou, I., and Serafeim, G. 2014. "Corporate Social Responsibility and Access to Finance," *Strategic management journal* (35:1), pp. 1-23.

Chevalier, J. A. 1995. "Capital Structure and Product-Market Competition: Empirical Evidence from the Supermarket Industry," *The American Economic Review* (85:3), pp. 415-435.

Cheynel, E. 2013. "A Theory of Voluntary Disclosure and Cost of Capital," *Review of Accounting Studies* (18:4), pp. 987-1020.

Chwelos, P., Ramirez, R., Kraemer, K. L., and Melville, N. P. 2010. "Research Note—Does Technological Progress Alter the Nature of Information Technology as a Production Input? New Evidence and New Results," *Information Systems Research* (21:2), pp. 392-408.

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.

Derrien, F., and Kecskés, A. 2013. "The Real Effects of Financial Shocks: Evidence from Exogenous Changes in Analyst Coverage," *The Journal of Finance* (68:4), pp. 1407-1440.

Dhaliwal, D. S., Li, O. Z., Tsang, A., and Yang, Y. G. 2011. "Voluntary Nonfinancial Disclosure and the Cost of Equity Capital: The Initiation of Corporate Social Responsibility Reporting," *The Accounting Review* (86:1), pp. 59-100.

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.

Dyer, T., Lang, M., and Stice-Lawrence, L. 2017. "The Evolution of 10-K Textual Disclosure: Evidence from Latent Dirichlet Allocation," *Journal of Accounting and Economics* (64:2-3), pp. 221-245.

Easley, D., and O'hara, M. 2004. "Information and the Cost of Capital," *The Journal of Finance* (59:4), pp. 1553-1583.

El Ghoul, S., Guedhami, O., Kwok, C. C., and Mishra, D. R. 2011. "Does Corporate Social Responsibility Affect the Cost of Capital?," *Journal of Banking & Finance* (35:9), pp. 2388-2406.

Faulkender, M., and Petersen, M. 2012. "Investment and Capital Constraints: Repatriations under the American Jobs Creation Act," *The Review of Financial Studies* (25:11), pp. 3351-3388.

Fazzini, K. 2018. "Moody's Is Going to Start Building the Risk of a Business-Ending Hack into Its Credit Ratings," in: *CNBC*.

Frank, M. Z., and Shen, T. 2016. "Investment and the Weighted Average Cost of Capital," *Journal of Financial Economics* (119:2), pp. 300-315.

Gao, C., Zuzul, T., Jones, G., and Khanna, T. 2017. "Overcoming Institutional Voids: A Reputation-Based View of Long-Run Survival," *Strategic Management Journal* (38:11), pp. 2147-2167.

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.

Greenwald, B. C., Stiglitz, J. E., and Weiss, A. 1984. "Informational Imperfections in the Capital Market and Macro-Economic Fluctuations." National Bureau of Economic Research Cambridge, Mass., USA.

Hail, L., and Leuz, C. 2006. "International Differences in the Cost of Equity Capital: Do Legal Institutions and Securities Regulation Matter?," *Journal of accounting research* (44:3), pp. 485-531.

Hall, B. H., and Lerner, J. 2010. "The Financing of R&D and Innovation," in *Handbook of the Economics of Innovation*. Elsevier, pp. 609-639.

Hassan, T. A., Hollander, S., van Lent, L., and Tahoun, A. 2019. "Firm-Level Political Risk: Measurement and Effects," *The Quarterly Journal of Economics* (134:4), pp. 2135-2202.

Havakhor, T., Sabherwal, R., Steelman, Z. R., and Sabherwal, S. 2019. "Relationships between Information Technology and Other Investments: A Contingent Interaction Model," *Information Systems Research* (30:1), pp. 291-305.

Heckman, J. J. 1979. "Sample Selection Bias as a Specification Error," *Econometrica* (47:1), pp. 153-161.

Hennessy, C. A., and Whited, T. M. 2007. "How Costly Is External Financing? Evidence from a Structural Estimation," *The Journal of Finance* (62:4), pp. 1705-1745.

Hoberg, G., and Phillips, G. 2010. "Product Market Synergies and Competition in Mergers and Acquisitions: A Text-Based Analysis," *The Review of Financial Studies* (23:10), pp. 3773-3811.

Hoberg, G., and Phillips, G. 2016. "Text-Based Network Industries and Endogenous Product Differentiation," *Journal of Political Economy* (124:5), pp. 1423-1465.

Hubbard, R. 1998. "Capital-Market Imperfections and Investment," *Journal of Economic Literature* (36:1), pp. 193-225.

Irvine, P. J. 2000. "Do Analysts Generate Trade for Their Firms? Evidence from the Toronto Stock Exchange," *Journal of Accounting and Economics* (30:2), pp. 209-226.

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.

Keen, P., and Williams, R. 2013. "Value Architectures for Digital Business: Beyond the Business Model," *MIS Quarterly* (37:2), pp. 643-647.

Khurana, I. K., and Raman, K. 2004. "Litigation Risk and the Financial Reporting Credibility of Big 4 Versus Non-Big 4 Audits: Evidence from Anglo-American Countries," *The Accounting Review* (79:2), pp. 473-495.

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.

Leeson, P. T., and Coyne, C. J. 2005. "The Economics of Computer Hacking," *Journal of Law, Economics and Policy* (1:2), pp. 511-532.

Li, F., Lundholm, R., and Minnis, M. 2013. "A Measure of Competition Based on 10-K Filings," *Journal of Accounting Research* (51:2), pp. 399-436.

Lintner, J. 1975. "Inflation and Security Returns," *The Journal of Finance* (30:2), pp. 259-280.

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.

Luo, X., Wang, H., Raithel, S., and Zheng, Q. 2015. "Corporate Social Performance, Analyst Stock Recommendations, and Firm Future Returns," *Strategic Management Journal* (36:1), pp. 123-136.

Malmendier, U., and Tate, G. 2009. "Superstar Ceos," *The Quarterly Journal of Economics* (124:4), pp. 1593-1638.

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.

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.

Mithas, S., Tafti, A., Bardhan, I., and Goh, J. M. 2012. "Information Technology and Firm Profitability: Mechanisms and Empirical Evidence," *MIS Quarterly*), pp. 205-224.

Mithas, S., Whitaker, J., and Tafti, A. 2017. "Information Technology, Revenues, and Profits: Exploring the Role of Foreign and Domestic Operations," *Information Systems Research* (28:2), pp. 430-444.

Mitra, S., and Chaya, A. K. 1996. "Analyzing Cost-Effectiveness of Organizations: The Impact of Information Technology Spending," *Journal of Management Information Systems* (13:2), pp. 29-57.

Myers, S. C., and Majluf, N. S. 1984. "Corporate Financing and Investment Decisions When Firms Have Information That Investors Do Not Have," *Journal of financial economics* (13:2), pp. 187-221.

Ofek, E. 1993. "Capital Structure and Firm Response to Poor Performance: An Empirical Analysis," *Journal of financial economics* (34:1), pp. 3-30.

Pagani, M. 2013. "Digital Business Strategy and Value Creation: Framing the Dynamic Cycle of Control Points," *Mis Quarterly*), pp. 617-632.

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.

Santhanam, R., and Hartono, E. 2003. "Issues in Linking Information Technology Capability to Firm Performance," *MIS Quarterly* (27:1), pp. 125-153.

Sharfman, M. P., and Fernando, C. S. 2008. "Environmental Risk Management and the Cost of Capital," *Strategic Management Journal* (29:6), pp. 569-592.

Sharpe, S. A. 1994. "Financial Market Imperfections, Firm Leverage, and the Cyclicality of Employment," *The American Economic Review* (84:4), pp. 1060-1074.

Shroff, N., Sun, A. X., White, H. D., and Zhang, W. 2013. "Voluntary Disclosure and Information Asymmetry: Evidence from the 2005 Securities Offering Reform," *Journal of Accounting Research* (51:5), pp. 1299-1345.

Singh, J. V., Tucker, D. J., and House, R. J. 1986. "Organizational Legitimacy and the Liability of Newness," *Administrative science quarterly*), pp. 171-193.

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.

Tambe, P. 2014. "Big Data Investment, Skills, and Firm Value," *Management Science* (60:6), pp. 1452-1469.

Tetlock, P. C. 2007. "Giving Content to Investor Sentiment: The Role of Media in the Stock Market," *The Journal of finance* (62:3), pp. 1139-1168.

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.

Womack, K. L. 1996. "Do Brokerage Analysts' Recommendations Have Investment Value?," *The journal of finance* (51:1), pp. 137-167.

Wooldridge, J. M. 2010. *Econometric Analysis of Cross Section and Panel Data*. MIT press.

Zhu, K. 2004. "The Complementarity of Information Technology Infrastructure and E-Commerce Capability: A Resource-Based Assessment of Their Business Value," *Journal of management information systems* (21:1), pp. 167-202.

Zuckerman, E. W. 2000. "Focusing the Corporate Product: Securities Analysts and De-Diversification," *Administrative Science Quarterly* (45:3), pp. 591-619.

Table 1. Variable definitions, measures, and data source

	Variable	Measure	Data Source
Dependent variables	Cost of Capital (WACC)	Weighted average cost of debt and cost of equity, where the latter is based on the Capital Asset Pricing Model (CAPM).	COMPUSTAT, Bloomberg financial
	Return on Assets (ROA)	Net income / total assets	COMPUSTAT
	Return on Sales (ROS)	Operating income / net sales	COMPUSTAT
	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
	Cost of Goods Sold (COGS)	All expenses directly allocated by the company to production, such as material, labor, and overhead.	COMPUSTAT
Independent variables	Disclosing Cybersecurity Investments (DCIs)	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
	Binary DCI *(robustness check)*	Equals 1 for firms that disclose at least one cybersecurity investment in their SEC filings in the current year, and 0 otherwise.	EDGAR
	Press Release Emphasis (PRE) *(robustness)*	Number of cybersecurity-related public press release/total number of public press releases	LexisNexis
Moderator	Informativeness	(Score 0-4)/4; scores based on whether the four characteristics of DCIs are present: $value, date of investment, projection it goes to effect, name of vendor/supplier/consultant name (technological investment) or name of startup/venture/R&D lab (innovation investment).	EDGAR
	Coverage	ln(1+number of analysts covering the firm)	IBES
Main Instrumental variables	Ind_Cyber_Breach	Industry averages of cybersecurity breaches	Privacy Rights Clearinghouse
	Ind_Cyber_Disclosure	Industry average of DCIs	EDGAR
	Ind _Cyber_Talent	Industry average number (ln(1+#)) of cybersecurity talent recruited	Proprietary online resume dataset
Control variables	Diversification	Entropy measure as outlined in Robins and Wiersema (1995)	COMPUSTAT
	Firm Size	ln(number of employees in thousands)	COMPUSTAT
	Assets	Total assets	COMPUSTAT
	R&D	R&D expenditure / annual revenue	COMPUSTAT
	Advertising (ADV)	Advertising expenditure / annual revenue	COMPUSTAT
	IT expenditure (IT_Exp)	Chwelos et al.'s (2010) measure of IT stock	CI Database
	Forecast error	The absolute difference between the latest analysts' median consensus forecasts before the earnings announcement and the firm's actual earning per share scaled by stock prices	IBES, CRSP
	Analysts' exposure	ln(1+number of years covering the firm)	IBES
	CSR disclosure	The number of public disclosures about their firm's socially responsible activities in CSR newswire	CSR newswire, Corporateregister.com
	Non-cyber disclosures	ln(# of non-cyber sentences in the SEC reports)	EDGAR
	SEC informativeness	ln(# of the number of informative numbers while dropping dates and section identifiers, etc.)	EDGAR

Table 2. Panel A. Correlation Table

	Variable	1	2	3	4	5	6	7	8	9	10	11	12	13
1	DCIs (%)													
2	Coverage	-0.09												
3	Informativeness	0.39	-0.02											
4	WACC	-0.19	0.04	-0.17										
5	IT_Exp	0.15	0.04	-0.03	-0.03									
6	Firm size	-0.03	0.09	0.01	0.06	0.19								
7	Assets	-0.14	0.10	0.00	0.04	0.14	0.25							
8	R&D	0.17	0.16	0.04	-0.10	0.17	0.31	0.07						
9	ADV	0.05	0.18	-0.06	-0.00	0.18	0.22	0.11	0.03					
10	Forecast error	0.02	-0.03	-0.08	0.03	0.05	-0.08	-0.07	0.25	0.03				
11	Analysts' exposure	0.01	0.05	0.03	-0.11	0.03	0.08	0.08	0.11	0.14	-0.12			
12	CSR	0.08	-0.04	-0.08	0.19	0.00	0.14	0.08	-0.09	0.20	0.05	0.08		
13	Non-cyber disc	-0.03	0.05	0.13	-0.04	-0.06	0.28	0.23	-0.12	0.11	-0.06	0.07	-0.06	
14	SEC inf.	0.11	-0.01	0.28	-0.22	-0.08	0.17	0.18	-0.08	0.14	-0.09	0.07	-0.15	0.08

Table 2. Panel B. Summary statistics and univariate comparisons

							DCI=0 N=4181		DCI>0 N=1877		
	Variable	Mean	S.D.	Median	Min	Max	Mean	S.D.	Mean	S.D.	t-diff
1	DCIs (%)	0.31	0.34	0.41	0	0.88	-	-	-	-	-
2	Coverage	0.98	0.91	0.95	0	1.79	0.990	0.919	0.951	0.892	1.56
3	Informativeness	0.03	0.37	0	0	1	0.000	0.000	0.230	0.374	-26.64***
4	WACC	0.08	0.09	0.06	0.005	0.28	0.083	0.088	0.078	0.089	2.03*
5	IT_Exp	0.03	0.06	0.04	0.003	0.11	0.029	0.059	0.033	0.082	-1.90#
6	Firm size	3.03	1.12	2.84	0.69	7.69	2.969	1.142	2.939	1.142	0.95
7	Assets	6.96	2.11	8.56	4.23	15.08	6.890	2.112	6.751	2.973	1.83#
8	R&D	0.08	0.16	0.07	0	0.66	0.073	0.157	0.086	0.282	-1.87#
9	ADV	0.02	0.12	0.03	0	0.16	0.020	0.122	0.021	0.122	-0.3
10	Forecast error	0.03	0.22	0.4	0.008	0.27	0.029	0.227	0.029	0.216	0
11	Analysts' exposure	1.42	1.02	1.37	0.69	2.079	1.40	1.06	1.44	1.01	-1.40
12	CSR	0.02	0.14	0	0	1	0.020	0.137	0.021	0.139	-0.26
13	Non-cyber disc.	8.16	1.76	7.23	6.93	8.89	8.323	1.707	8.242	1.707	1.71
14	SEC inf.	7.13	1.09	7.16	6.25	8.25	7.126	1.182	7.157	1.112	-0.98

Notes. DCIs stands for disclosing cybersecurity investments, IT_Exp for IT expenditure, ADV for advertising expenditure, ROA for return on assets, ROS for return on sales, WACC for cost of capital, CSR for corporate social responsibility,and SEC info for SEC informativeness.

Table 3. Main results

DV= Cost of Capital	FE (1)	2SLS+FE (2)	2SLS+FE (3)	2SLS+FE (4)
DCIs	-0.155***	-0.121***	-0.103***	-0.084***
	(0.032)	(0.028)	(0.028)	(0.023)
Coverage			-0.01	-0.01
			(0.006)	(0.007)
Informativeness			-0.009	-0.011
			(0.008)	(0.007)
Coverage×DCIs				-0.034#
				(0.018)
Informativeness×DCIs				-0.044*
				(0.021)
Firm size	0.002	0.002	0.002	0.002
	(0.001)	(0.002)	(0.002)	(0.001)
Assets	0.005	0.005	0.005	0.005
	(0.004)	(0.004)	(0.004)	(0.003)
Diversification	0.001	0.001	0.001	0.001
	(0.001)	(0.001)	(0.001)	(0.001)
R&D	-0.255***	-0.169***	-0.203***	-0.136***
	(0.05)	(0.032)	(0.043)	(0.022)
ADV	0.003	0.003	0.003	0.003
	(0.002)	(0.002)	(0.003)	(0.002)
IT_Exp	-0.062*	-0.041#	-0.026	-0.042*
	(0.031)	(0.023)	(0.02)	(0.017)
Forecast error	0.005	0.005	0.005	0.005
	(0.004)	(0.003)	(0.004)	(0.004)
Analyst exposure	0.009	0.01	0.01	0.009
	(0.006)	(0.008)	(0.009)	(0.007)
CSR	-0.186***	-0.228***	-0.242***	-0.249***
	(0.035)	(0.063)	(0.054)	(0.037)
Non-cyber disc.	-0.010	-0.011	-0.009	-0.01
	(0.007)	(0.007)	(0.006)	(0.007)
SEC informativeness	-0.012	-0.009	-0.009	-0.01
	(0.008)	(0.007)	(0.006)	(0.006)
Wald's Chi	14350.05	11387.2	12801.8	11728.61
Fixed Effects	YES	YES	YES	YES
YEAR-Ind dummies	YES	YES	YES	YES
# of Firms	6,058	6,058	6,058	6,058
Observations	74,755	74,755	74,755	74,755

Notes. DCIs stands for disclosing cybersecurity investments, IT_Exp for IT expenditure, and ADV for advertising expenditure, CSR for corporate social responsibility. For ease of interpretation, all continuous variables are standardized. Standard errors are in parentheses. Out of 6,058 firms in the sample, 1,877 firms (30.98%) had at least one report with a confirmed DCI.***p < 0.001; **p < 0.01; *p < 0.05; # p < 0.10.

Table 4. Robustness checks: alternative measures for DCIs, cost of capital, and analyst coverage

	DCIs (Binary)	DCIs (10-k's only)	DCIs (Press Release)	Alternative Outcomes			Expert coverage
DV =	Cost of Capital	Cost of Capital	Cost of Capital	Cost of Debt	Cost of Equity	Cost of Capital (FF3M)	Cost of Capital
	(1)	(2)	(3)	(4)	(5)	(6)	(7)
DCIs	-0.101***	-0.091***	-0.091***	-0.075***	-0.135***	-0.087***	-0.102***
	(0.025)	(0.027)	(0.027)	(0.019)	(0.029)	(0.016)	(0.025)
Coverage	-0.011	-0.011	-0.009	-0.010	-0.011	-0.008	-0.016*
	(0.009)	(0.007)	(0.006)	(0.009)	(0.009)	(0.005)	(0.007)
Informativeness	-0.009	-0.011	-0.010	-0.010	-0.010	-0.004	-0.011
	(0.005)	(0.009)	(0.006)	(0.007)	(0.008)	(0.003)	(0.009)
Coverage×DCIs	-0.031	-0.032*	-0.028*	-0.032*	0.041**	-0.034#	-0.086**
	(0.025)	(0.016)	(0.011)	(0.014)	(0.014)	(0.019)	(0.033)
Informativeness×DCIs	-0.056*	-0.052*	-0.043*	-0.05*	-0.044*	-0.05*	-0.055*
	(0.023)	(0.025)	(0.021)	(0.024)	(0.021)	(0.021)	(0.027)
Firm size	0.002	0.002	0.002	0.002	0.002	0.002	0.002
	(0.001)	(0.001)	(0.002)	(0.001)	(0.002)	(0.002)	(0.001)
Assets	0.005	0.005	0.005	0.005	0.006	0.005	0.005
	(0.003)	(0.003)	(0.004)	(0.003)	(0.005)	(0.004)	(0.004)
Diversification	0.001	0.001	0.001	0.001	0.001	0.001	0.001
	(0.001)	(0.001)	(0.001)	(0.001)	(0.001)	(0.001)	(0.001)
R&D	-0.158***	-0.163***	-0.15***	-0.118***	-0.138***	-0.174***	-0.178***
	(0.028)	(0.046)	(0.025)	(0.02)	(0.027)	(0.043)	(0.039)
ADV	0.003	0.003	0.003	0.003	0.003	0.003	0.003
	(0.002)	(0.002)	(0.002)	(0.002)	(0.002)	(0.002)	(0.002)
IT_Exp	-0.034#	-0.043*	-0.044*	-0.039#	-0.045*	-0.044*	-0.042*
	(0.019)	(0.017)	(0.018)	(0.022)	(0.019)	(0.018)	(0.018)
Forecast error	0.005	0.005	0.006	0.004	0.005	0.005	0.005
	(0.003)	(0.004)	(0.005)	(0.003)	(0.003)	(0.003)	(0.004)
Analyst exposure	0.009	0.010	0.010	0.009	0.010	0.009	0.011
	(0.007)	(0.006)	(0.007)	(0.007)	(0.007)	(0.008)	(0.009)
CSR	-0.244***	-0.187***	-0.233***	-0.158***	-0.249***	-0.211***	-0.162***
	(0.037)	(0.032)	(0.038)	(0.029)	(0.042)	(0.038)	(0.041)
Non-cyber disc.	-0.011	-0.009	-0.011	-0.010	-0.011	-0.010	0.000
	(0.007)	(0.007)	(0.007)	(0.006)	(0.009)	(0.009)	(0.004)
SEC informativeness	-0.012	-0.012	-0.011	-0.009	-0.010	0.002	-0.009
	(0.008)	(0.008)	(0.007)	(0.008)	(0.006)	(0.001)	(0.008)
Wald's Chi	12525.7	12525.7	11842.48	11956.35	11728.61	12753.44	13074.67
Fixed Effects	YES	YES	YES	YES	YES	YES	YES
YEAR-Ind dummies	YES	YES	YES	YES	YES	YES	YES
# of Firms	6,058	6,058	6,058	6,058	6,058	6,058	6,058
Observations	74,755	74,755	74,755	74,755	74,755	74,755	74,755

Notes. DCIs stands for disclosing cybersecurity investments, IT_Exp for IT expenditure, and ADV for advertising expenditure, CSR for corporate social responsibility, and FF3M for Fama-French 3-factor model. For ease of interpretation, all continuous variables are standardized. Standard errors are in parentheses. ***p < 0.001; **p < 0.01; *p < 0.05; # p < 0.10.

Table 5. Falsification tests

DV=	Cost of Capital (1)	Cost of Goods Sold (2)
DCIs		-0.009
		(0.006)
DCRs	-0.013	
	(0.01)	
Coverage	-0.009	-0.008
	(0.007)	(0.006)
Informativeness	-0.005	-0.004
	(0.004)	(0.003)
Coverage×DCIs		-0.012
		(0.018)
Informativeness×DCIs		-0.005
		(0.021)
Coverage×DCRs	-0.005	
	(0.014)	
Informativeness×DCRs	-0.015	
	(0.024)	
Firm size	0.002	-0.035#
	(0.001)	(0.02)
Assets	0.005	0.005
	(0.003)	(0.003)
Diversification	0.001	0.001
	(0.001)	(0.001)
R&D	-0.171***	-0.037#
	(0.037)	(0.022)
ADV	0.003	0.003
	(0.002)	(0.002)
IT_Exp	-0.044*	-0.099***
	(0.021)	(0.03)
Forecast error	0.004	0.006
	(0.003)	(0.004)
Analyst exposure	0.009	0.011
	(0.006)	(0.008)
CSR	-0.242***	0.016
	(0.038)	(0.01)
Non-cyber disc.	-0.011	0.009
	(0.01)	(0.007)
SEC informativeness	0.001	0.008
	(0.001)	(0.006)
Wald's Chi	10362.17	11614.74
Fixed Effects	YES	YES
YEAR-Ind dummies	YES	YES
# of Firms	6,058	6,058
Observations	74,755	74,755

Notes. DCIs stands for disclosing cybersecurity investments, DCRs for disclosing cybersecurity risks, IT_Exp for IT expenditure, and ADV for advertising expenditure, CSR for corporate social responsibility. For ease of interpretation, all continuous variables are standardized. Standard errors are in parentheses. ***p < 0.001; **p < 0.01; *p < 0.05; # p < 0.10.

Table 6. Further Identification Improvements

DV= Cost of Capital	Analyst coverage instrumented	Exclusion controls added	Firm IT sec Inv.
	(1)	(2)	(3)
DCIs	-0.108*** (0.026)	-0.122*** (0.02)	-0.105*** (0.018)
Breach		0.232*** (0.067)	
Talent		-0.008 (0.006)	
Coverage	-0.016 (0.012)	-0.009 (0.005)	-0.012 (0.009)
Informativeness	-0.005 (0.004)	-0.002 (0.002)	-0.004 (0.003)
Coverage×DCIs	-0.075*** (0.017)	-0.021# (0.012)	-0.048* (0.02)
Informativeness×DCIs	-0.049* (0.021)	-0.028* (0.014)	-0.051* (0.021)
Firm size	0.002 (0.001)	0.006 (0.004)	0.002 (0.001)
Assets	0.006 (0.004)	0.004 (0.003)	0.005 (0.004)
Diversification	0.001 (0.001)	0.003 (0.002)	0.001 (0.001)
R&D	-0.142*** (0.039)	-0.218*** (0.056)	-0.149*** (0.026)
ADV	0.003 (0.002)	0.005 (0.004)	0.003 (0.002)
IT_Exp	-0.041# (0.022)	-0.038* (0.019)	-0.036# (0.021)
Forecast error	0.004 (0.003)	0.006 (0.004)	0.005 (0.004)
Analyst exposure	0.011 (0.008)	0.009 (0.006)	0.009 (0.007)
CSR	-0.194*** (0.04)	-0.205*** (0.034)	-0.231*** (0.055)
Non-cyber disc.	-0.011 (0.008)	-0.011 (0.01)	-0.009 (0.007)
SEC informativeness	0.004 (0.003)	-0.002 (0.002)	0.008 (0.005)
Wald's Chi	12753.44	16203.74	83940.9
Fixed Effects	YES	YES	YES
YEAR-Ind dummies	YES	YES	YES
# of Firms	6,058	6,058	4,716
Observations	74,755	74,755	28,842

Notes. DCIs stands for disclosing cybersecurity investments, IT_Exp for IT expenditure, and ADV for advertising expenditure, CSR for corporate social responsibility. For ease of interpretation, all continuous variables are standardized. The coefficients of 14 controls pertaining to IT security investments in Column 3 are omitted from the table for brevity. Standard errors are in parentheses. ***p < 0.001; **p < 0.01; *p < 0.05; # p < 0.10.

Table 7. Complimentary Identification Approach: Difference-in-differences

DV=	Cost of Capital (1)	Cost of Capital (2)
Treat×Post	-0.087*** (0.015)	
Placebo×Post		-0.009 (0.008)
Post	0.003 (0.002)	0.002 (0.001)
IMR	0.01 (0.006)	0.008 (0.005)
Wald's Chi	4806.88	5804.24
Control	YES	YES
Fixed Effects	YES	YES
YEAR-IND	YES	YES
# of Firms	348	568
Observations	696	1136

Notes. $treat_i = 1$ if firm i had one or more DCI(s) in the sample period, 0 otherwise. $post_{it} = 1$ if firm i had one or more DCI(s) on or before year t, 0 otherwise. $placebo_{it} = 1$ if firm i had one or more discussions of cybersecurity risks without pointing to a tangible cybersecurity investment on or before year t, 0 otherwise. IMR stands for Inverse Mills Ratio. ***p < 0.001; **p < 0.01; *p < 0.05; # p < 0.10.

Table 8. Additional Analyses

DV =	Tobin's q (1)	ROA_t (2)	ROA_{t+1} (3)	ROA_{t+2} (4)	ROS_t (5)	ROS_{t+1} (6)	ROS_{t+2} (7)
DCIs	0.109*** (0.026)	-0.011 (0.008)	0.028 (0.019)	0.048* (0.024)	-0.01 (0.008)	0.019 (0.014)	0.063* (0.026)
Firm size	0.043* (0.022)	0.021 (0.014)	0.023 (0.015)	0.017 (0.012)	0.021 (0.018)	0.019 (0.015)	0.028 (0.025)
Assets	0.171*** (0.037)	0.069** (0.026)	0.052* (0.022)	0.055* (0.022)	0.056* (0.028)	0.064** (0.021)	0.040# (0.023)
Diversification	0.008 (0.006)	0.003 (0.002)	0.003 (0.002)	0.003 (0.002)	0.001 (0.001)	-0.005 (0.004)	0.005 (0.004)
R&D	0.227*** (0.056)	0.02 (0.016)	0.021 (0.013)	0.091*** (0.014)	0.018 (0.012)	0.02 (0.012)	0.087*** (0.017)
ADV	0.28*** (0.06)	0.074*** (0.014)	0.078*** (0.018)	0.064** (0.021)	0.078*** (0.015)	0.079*** (0.021)	0.071** (0.025)
IT_Exp	0.071** (0.025)	-0.009 (0.007)	0.024 (0.019)	0.058* (0.028)	-0.01 (0.007)	0.026 (0.017)	0.045 (0.02)
Wald's Chi	9046.42	1170.72	2562.15	2536.11	1179.78	3272.48	2635.36
Fixed Effects	YES	YES	YES	YES	YES	YES	YES
YEAR-Ind	YES	YES	YES	YES	YES	YES	YES
# of Firms	6,058	6,058	6,058	6,058	6,058	6,058	6,058
Observations	74,755	74,755	74,755	74,755	74,755	74,755	74,755

Notes. DCIs stands for disclosing cybersecurity investments, IT_Exp for IT expenditure, ADV for advertising expenditure, ROA for return on assets, and ROS for return on sales. For ease of interpretation, all continuous variables are standardized. Standard errors are in parentheses. ***p < 0.001; **p < 0.01; *p < 0.05; # p < 0.10.

Appendix A: Keywords List

Keywords used to find cybersecurity investments[18]	Keywords used to find cybersecurity talent
Cyber/digital/computer/information/data Authentication	Cyber/digital/computer/information/data Authentication
Access control	Access control
Computer security	Computer security
Computer virus	Computer virus detection/protection/defense
Cyber fraud	Cyber fraud detection/protection/defense
Cyber investigation	Cyber investigation
Cyber operation	Cyber operation
Cyber/digital/computer break-in	Cyber/digital/computer break-in detection/protection/defense
Cyber/digital/computer/information/data attack	Cyber/digital/computer/information/data attack detection/protection
Cyber/digital/computer/information/data defense	Cyber/digital/computer/information/data defense
Cyber/digital/computer/information/data protection	Cyber/digital/computer/information/data protection
Cyber/digital/computer/information/data theft	Cyber/digital/computer/information/data theft detection/protection/defense
Cyber/digital/computer/information/data threat	Cyber/digital/computer/information/data threat detection/protection/defense
Cyber/digital/computer/information/data vulnerability	Cyber/digital/computer/information/data vulnerability detection/protection/defense
Cyber/digital/computer/information/data vulnerability assessment	Cyber/digital/computer/information/data vulnerability assessment
Cyber/digital/computer/network intrusion	Cyber/digital/computer/network intrusion detection/protection/defense
Cyber/Security assessment	Cyber/Security assessment
Cyber/security investment/expenditure	-
Cybersecurity breach	Cybersecurity breach detection/protection/defense
Cyberspace	Cyberspace
Data breach	Data breach detection/protection/defense
Denial of service	Denial of service detection/protection/defense
Digital forensics	Digital forensics
Disaster recovery	Disaster recovery
Encryption	Encryption
Exploitation analysis	Exploitation analysis
Firewall	Firewall
Hack	Hack/ing detection/protection/defense
Identity theft	Identity theft detection/protection/defense
Information security breach	Information security breach detection/protection/defense
Infosec	Infosec
Phishing	Phishing detection/protection/defense
Privacy breach	Privacy breach detection/protection/defense
Security breach	Security breach detection/protection/defense

[18] The keywords are only used for initial selection of reports and the final categorization into a DCI is done *manually*, as explained in the section 3.1.

Appendix B. Measurement of cybersecurity talent recruitment

The cybersecurity talent recruitment in industry firms is measured by the natural log of the sum+1 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.[19] The information about the recruitment of employees is extracted from the employees' posted resumes (i.e., from the database of 70 million resumes). 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. The natural log of weighted sum (weighted by years of experience in a cybersecurity project/position prior to recruitment) of total hits for such a search is then treated at talent recruitment for Target Inc. in 2013.[20]

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, the identified sections of all the available resumes were searched to find matches with the

[19] 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 this main measure show better fit indices, perhaps due to 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.

[20] 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.

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 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 an input to a machine learning algorithm (Bai et al. 2004) (see section 4.3. of Bai et al. 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.

Appendix C. First stage of the 2SLS estimations

Table C1. First stage estimation

DV=	DCIs	DCIs	Informativeness×DCIs	Coverage×DCIs
	(1)	(2)	(3)	(4)
Ind_Cyber_Breach	0.378*** (0.071)	0.548*** (0.091)	0.232*** (0.05)	0.184*** (0.047)
Ind_Cyber_Disclosure	0.36*** (0.067)	0.303*** (0.055)	0.403*** (0.109)	0.275*** (0.055)
Ind_Cyber_Talent	0.326*** (0.071)	0.468*** (0.098)	0.197*** (0.059)	0.233*** (0.055)
Ind_Cyber_Breach×Informativeness		0.012 (0.008)	0.364*** (0.103)	0.014 (0.009)
Ind_Cyber_Disclosure×Informativeness		0.005 (0.003)	0.257*** (0.075)	0.004 (0.002)
Ind_Cyber_Talent×Informativeness		0.006 (0.004)	0.32*** (0.067)	0.004 (0.003)
Ind_Cyber_Breach×Coverage		0.014 (0.01)	0.012 (0.008)	0.275*** (0.08)
Ind_Cyber_Disclosure×Coverage		0.005 (0.004)	0.007 (0.005)	0.268*** (0.065)
Ind_CyberTalent×Coverage		0.005 (0.003)	0.006 (0.004)	0.361*** (0.055)
Adj. R-Squared	0.62	0.68	0.66	0.65
Firm controls	YES	YES	YES	YES
# of Firms	6,058	6,058	6,058	6,058
Observations	74,755	74,755	74,755	74,755

Notes. Ind_Cyber_Breach stands for industry averages of cybersecurity breaches, Ind_Cyber_Disclosures for industry averages of DCIs, Ind_Cyber_Talent for industry average number of cybersecurity talent. ***p < 0.001; **p < 0.01; *p < 0.05; # p < 0.10.

Appendix D. Relative time DID estimation

Table D1. Relative Time DID

DV=	Cost of Capital
Rel_Time (t-3)×Treat	0.007 (0.005)
Rel_Time (t-2)×Treat	0.012 (0.009)
Rel_Time (t-1)×Treat	Omitted
Rel_Time (t0)×Treat	-0.092*** (0.022)
Rel_Time (t+1)×Treat	-0.061* (0.026)
Rel_Time (t+2)×Treat	-0.034# (0.019)
Firm Control	YES
Firm FE	YES
Year FE	YES
Wald's Chi	3892.24
# of Firms	348
Observations	2,088

$Rel\_Time(t-i) = 1$ if the firm had one or more DCI(s) i years until year t, 0 otherwise. $treat_i = 1$ if firm i had one or more DCI(s) in the sample period, 0 otherwise. ***p < 0.001; **p < 0.01; *p < 0.05; # p < 0.10.