Information Systems Research

Publication details, including instructions for authors and subscription information:
http://pubsonline.informs.org

Disclosure of Cybersecurity Investments and the Cost of Capital

Taha Havakhor, Mohammad S. Rahman, Tianjian Zhang

To cite this article:
Taha Havakhor, Mohammad S. Rahman, Tianjian Zhang (2026) Disclosure of Cybersecurity Investments and the Cost of Capital. Information Systems Research

Published online in Articles in Advance 20 Apr 2026

. https://doi.org/10.1287/isre.2023.0260

https://pubsonline.informs.org/journal/isre

INFORMATION SYSTEMS RESEARCH
Articles in Advance, pp. 1–23
ISSN 1047-7047 (print), ISSN 1526-5536 (online)

Disclosure of Cybersecurity Investments and the Cost of Capital

Taha Havakhor,[a] Mohammad S. Rahman,[b,*] Tianjian Zhang[c]

[a] Desautels Faculty of Management, McGill University, Montreal, Quebec H3A 0G4, Canada; [b] Mitch Daniels School of Business, Purdue University, West Lafayette, Indiana 47907; [c] College of Business Administration and Public Policy, California State University–Dominguez Hills, Carson, California 90747

*Corresponding author

Contact: taha.havakhor@mcgill.ca, https://orcid.org/0000-0002-4338-5970 (TH); mrahman@purdue.edu, https://orcid.org/0000-0003-2115-5776 (MSR); tzhang@csudh.edu, https://orcid.org/0000-0003-1035-2838 (TZ)

Received: April 28, 2023
Revised: January 27, 2024; November 11, 2024; May 24, 2025
Accepted: August 9, 2025
Published Online in Articles in Advance: April 20, 2026

https://doi.org/10.1287/isre.2023.0260

Abstract. Despite investor interest and continued encouragement of transparency by regulators, firms generally adopt a private stance and refrain from disclosing investments in cybersecurity countermeasures. Existing literature suggests that firms may lack sufficient incentives to offset the potential risks of such disclosures. Thus, in the absence of clear evidence capturing robust benefits, firms may remain disincentivized to disclose their cybersecurity investments. Using exogenous shocks triggered by the U.S. Securities and Exchange Commission comment letters, this study investigates one strong incentive for disclosure: improved access to capital. We find that firms disclosing cybersecurity investments experience a significant reduction in their cost of accessing debt and equity capital and thus in their overall cost of capital. Further, we unravel the information intermediation process that is activated by signals sent through cybersecurity investment disclosures and leads to subsequent easier access to capital. Specifically, we show that disclosing firms with fewer boilerplate statements, that is, more informative ones, and those with higher analyst coverage or institutional ownership reap the highest benefits. Consistent with an information intermediation mechanism, which involves further information discovery by intermediaries, we demonstrate that actual investments in cybersecurity also strengthen the link between disclosure and cost of capital. This study reveals a robust and stable financial benefit of transparency in cybersecurity management, which transcends the transitory and sentimental short-term price variation impacts. This discovery encourages firms to proactively disclose their investments and mitigate information asymmetries related to their cybersecurity activities in an increasingly risky environment.

History: Bin Gu, Senior Editor; Idris Adjerid, Associate Editor.

Supplemental Material: The online appendices are available at https://doi.org/10.1287/isre.2023.0260.

Keywords: disclosure • cybersecurity investment • cost of capital • informativeness of disclosure • analyst coverage

1. Introduction

In today's digital economy, the threat of cyberattacks looms large, prompting an increase in cybersecurity spending to mitigate these risks. A recent report projects that global spending on cybersecurity products and services will reach $212 billion in 2025,[1] reflecting the growing awareness and response to these threats. Despite these significant investments, there remains a notable gap in public disclosure about these expenditures, particularly in annual reports. Although the U.S. Securities and Exchange Commission (SEC) issued guidance in 2011 and 2018 to encourage clearer communication of cyber risks,[2] disclosures of cybersecurity investments (DCI) remain scant.[3] The latest 2023 SEC rules on disclosing risk management practices further tighten the requirements,[4] highlighting the ongoing scarcity of voluntary disclosures despite past regulatory efforts. The reason for this lack of disclosure might be that, in the absence of evidence showing a tangible payoff, firms may consider nondisclosure the safer option.

Disclosing cybersecurity investments involves unique tradeoffs. On the one hand, several disincentives discourage firms from disclosures. One significant concern is the potential litigation risks (Cutler et al. 2019). Public disclosures about cybersecurity strategies can expose companies to legal challenges, especially if the disclosed information is later used against them in lawsuits. For instance, if a company discloses cybersecurity investments and still suffers a breach, plaintiffs could argue

that the company's disclosed investments were inadequate, leading to legal and financial repercussions.[5] Disclosures may also reveal competitive disadvantages. Although cybersecurity investments typically reduce cyber risks (Kwon and Johnson 2014, Angst et al. 2017), disclosing them can invite scrutiny from stakeholders and regulators. Stakeholders might deem the disclosed efforts insufficient or believe that excessive investment in cybersecurity could erode the firm's profitability. These stakeholders may ask about the unintended effects of the underlying investments: is the firm in trouble or facing undisclosed risks? Or has the firm, following industrial fads, over-invested in cybersecurity, which could negatively impact its profit margins? Without regulatory requirements, firms may prefer not to disclose cybersecurity investments to avoid the potential negative reactions and consequences (Bertomeu et al. 2021).

On the other hand, DCIs can, at least in theory, carry some rewards for the firm. DCIs signal reduced firm risks to the market, because publicly sharing cybersecurity efforts can demonstrate a proactive stance on risk management. This transparency can enhance a firm's reputation and potentially lead to a higher market valuation, with stakeholders viewing the firm as less risky. Additionally, disclosing cybersecurity investments may attract and retain customers and suppliers who prioritize data security. Given that data breaches can negatively impact sales (Kamiya et al. 2021), transparency in cybersecurity efforts can be appealing to consumers seeking companies that actively protect their data. Moreover, anecdotal evidence suggests that discretionary disclosure of cybersecurity investments may have payoffs. For example, Moody's Investor Service has started to incorporate cybersecurity risks in firms' credit ratings (Fazzini 2018). As Moody's managing director Derek Vadala stated (March 4, 2019), "We view cyber risk as event risk that can have a material impact on sectors and individual issuers." Empirical evidence also suggests that security breaches can affect firms' financing costs and market valuations (Huang and Wang 2020, Kamiya et al. 2021).

However, the realization of rewards for signaling DCIs is not always guaranteed. There are cases where markets are unresponsive to data breaches (Kvochko and Pant 2015, Foerderer and Schuetz 2022), and certain consumers prioritize convenience over data security (Agarwal et al. 2024). The inconsistency in market and consumer responses to security measures creates uncertainty about the lasting rewards of disclosing cybersecurity investments, leaving firms to question the overall value of transparency in this area. Given the numerous disincentives and the uncertain rewards of disclosing cybersecurity investments, it becomes imperative to investigate fundamental economic benefits that may concretely incentivize disclosure decisions.

One aspect that can help reduce uncertainty around the benefits of disclosure is understanding whether and how market rewards can be realized after revealing their cybersecurity efforts. Although such disclosures do not directly disclose risks, the underlying cybersecurity investments can reduce the risk of data breaches (Wang et al. 2013, Kwon and Johnson 2014, Angst et al. 2017). Financial market literature indicates that investors reward disclosure of factors that mitigate firm risk by lowering the cost of capital (Francis et al. 2008, Dhaliwal et al. 2011). Because the cost of capital reflects firms' risk profiles, information about investments that mitigate cyber risks should be a relevant component in its determination. However, without robust investigations, it remains unclear whether and to what extent financial markets consider disclosures about cybersecurity investments relevant to firm risk and whether such disclosures actually result in a lower cost of capital. This study intends to bring clarity to this question.

Cost of capital represents the rate of return a company must achieve to justify the financial risk of its investments and maintain its market value. It reflects a firm's ability to access capital and serves as the threshold return necessary to compensate investors (both debt holders and equity shareholders) for the risk they assume by providing capital (Easley and O'Hara 2004). Essentially, it serves as a benchmark for making investment decisions. Specifically, we focus on the cost of capital because it is closely tied to the risk associated with a firm's operations and capital structure. Investors demand higher returns for greater risks: The riskier a firm is, whether due to volatile earnings, uncertain cash flows, high debt levels, or operations threats, the higher its cost of capital. Both debt and equity investors expect higher returns to compensate for these risks, making the cost of capital a reflection of the overall risk the firm poses to its financiers (Verrecchia 2001). Because cybersecurity investments are meant to curb operational risks, cost of capital is a particularly relevant outcome to examine.

Beyond its relevance to cybersecurity investments, cost of capital offers several advantages over the usually analyzed cumulative abnormal returns (CAR). First, although CAR is often influenced by short-term market conditions, investor sentiment, and other external factors (Chan 2003), cost of capital is rooted in a firm's financial (including debt) structure. Although useful for assessing immediate market reaction, CAR might not provide a reliable metric for long-term decision making and therefore appears transitory for managers who may need a more robust incentive to disclose cybersecurity investments. Second, cost of capital offers a more comprehensive view of risk as perceived by a firm's capital investors. Commonly referred to as the weighted average cost of capital

(WACC), cost of capital combines both cost of debt and cost of equity, weighted according to the proportion of each in the company's capital structure. Debt and equity entail different risks and costs (Marsh 1982). The cost of debt is generally lower because it is less risky than equity (as debt holders have priority in case of bankruptcy), and interest on debt is tax deductible, reducing the effective cost. In contrast, equity investors request a higher return because they bear greater risk (being last in line for claims on assets and earnings). By accounting for both equity and debt in the cost of capital, WACC captures the overall risk and return expectations of a company's financing sources, thereby providing a more holistic view of a company's financing costs and risk profile.

To empirically test the impact of disclosing cybersecurity investments on the cost of capital, we analyze a sample of public firms and their disclosed cybersecurity investments based on SEC filings. Our sample consists of 16,680 firm-year observations of 1,933 firms spanning from 2006 to 2018. We find a persistent and robust impact from DCI on the cost of equity, cost of debt, and importantly, the overall cost of capital. We triangulate our estimates through multiple identification strategies (instrumentation using comment letters (CLs) issuance, Hausman-type instruments, and a difference-in-differences (DID) estimation using peer incidents as external shocks), along with falsification tests, tests of mechanism, and various robustness tests.

Turning to the mechanism underlying the key link established above, we first theorize that because disclosures in periodic reports like 10-K are usually brief, DCIs *act as signals* that impact the cost of capital through an information intermediation process performed by intermediaries such as analysts (Healy and Palepu 2001, Blankespoor et al. 2020). By definition, signals are snippets of information that a firm provides to indicate its financial health, strategic direction, or future prospects, inviting analysts to pay closer attention and investigate further (Easley and O'Hara 2004). We theorize that DCIs capture the attention of these information intermediaries, who are tasked with parsing these signals and expanding on matters discussed in periodic disclosures. These intermediaries often have access to proprietary tools to further understand the nature of investments made and measures taken by the firm. As such, DCIs that can stand out, DCIs by firms more exposed to information intermediation, and DCIs that are better backed by actual investments in cybersecurity are met with a higher reduction in cost of capital. Consistent with the theorization, we find that the impact of a firm's DCI on its cost of capital is greater when (a) the firm's DCIs stand out relative to its industry peers and its own history, (b) more analysts cover (and interpret) the firm's activities and the firm's stock is traded by institutional investors, and (c) the firm invests more substantially in cybersecurity.

Taken together, this study unravels a unique discovery beyond short-term equity-market reactions documented in prior studies (Gordon et al. 2010, Bose and Leung 2019) and reveals several boundary conditions that determine how disclosures of cybersecurity investment reduce firms' perceived risks and improve their access to capital. Our study offers fresh insights into how signals conveyed through disclosures of cybersecurity investments undergo an information intermediation process, ultimately facilitating better access to capital.

2. Theoretical Development

2.1. Cost of Capital, Risk Assessment, and Information Asymmetry

Cost of capital is fundamental to various firm activities, including investments in growth and survival projects, and is closely tied to firm profitability (Easley and O'Hara 2004). Financially constrained organizations, that is, those with a high cost of capital, tend to scale back their strategic activities (Hubbard 1998), including their investments in research and development (R&D; Hall and Lerner 2010). Moreover, access to capital is critical for firm survival as financing frictions can force a firm to forgo investment opportunities with a positive net present value (NPV) 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 *information asymmetries* between investors and the firm create imperfections, causing the supply curve to slope upward (Hennessy and Whited 2007). In other words, for investors, borrowing firms are heterogeneous in terms of their payback and growth ability; that is, they are heterogeneous in terms of the investment risk they pose. For that reason, 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 engage in actions that increase transparency and reduce information asymmetry (Verrecchia 2001, Easley and O'Hara 2004). To this end, firms may implement high-quality accounting standards (Barth et al. 2013) and voluntarily disclose critical firm activities (Shroff et al. 2013). Moreover, firms may solicit the services of business analysts to monitor firm activities (usually at the request of investment banks).

As investors base their assessment of a borrowing firm on its fundamental value, factors contributing to the borrower's business risks are of paramount

importance in shaping investors' perceptions of investment risk (Cheng et al. 2014). Therefore, although transparency about potential risks is a necessary condition to reduce information asymmetries in capital markets, the conveyed information to investors should also increase their positive evaluation of the fundamental value of the firm. For instance, optimism in analysts' forecasts has been shown to reduce the friction 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 for a business. The existing literature in strategic management (Sharfman and Fernando 2008) and corporate finance (Dhaliwal et al. 2011) has been consistent in showing that firms with reduced legal and market risks benefit from a significantly lower cost of capital, especially when the organizational measures in cutting those risks are disclosed by the firm (Dhaliwal et al. 2011) and externally monitored by analysts (Luo et al. 2015).

2.2. Cybersecurity 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, erode reputation, can lead to litigation and fines, and may force firms to engage in strategic shifts to remediate the damage (Kamiya et al. 2021). With their extended impact on the broader operations and survival of the firm, cybersecurity breaches and failures pose particular risks, that is, cybersecurity risks, which can impact the fundamental value of a firm. If financial markets, when unprompted, do not consider—or significantly underestimate—cybersecurity risks, then managers will remain unmotivated to reveal such information. The behavioral theory of the firm has amassed considerable evidence (Argote and Greve 2007) suggesting that managers often respond to problems reactively (i.e., problematic search) rather than proactively. Also, existing research shows that fear of increased market scrutiny is a likely reason for nondisclosure (Marquis et al. 2016), thereby implying that managers believe that disclosures of cybersecurity investments can invite unwanted scrutiny that negates the very purpose of such disclosures.

On the other hand, the evidence tilts more heavily toward supporting the assumption that financial markets already price cybersecurity risks. Empirical evidence shows that a firm's vulnerability to cybersecurity risks is part of the estimation of the firm's fundamental value (Kamiya et al. 2021). Moreover, anecdotal evidence supports the significance of cybersecurity damage to a firm's fundamental value and the subsequent reaction by investors as is exemplified in a Standard and Poor's report downgrading the rating forecast of Equifax Inc. to negative following the announcement of its data breach 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.

As such, cybersecurity risks are under the radar of investors, at least to some degree. If financial markets assume that firms are vulnerable to cybersecurity risks and price an average cybersecurity risk cost for all firms, then firms that invest in cybersecurity protection but do not disclose these investments may nevertheless be overcharged by the financial markets. Therefore, it can be argued that unless firms inform the market of their cybersecurity preparedness, their cybersecurity risks may remain overpriced. Empirical studies on cybersecurity investments have documented the preventive value by examining their impact in reducing a firm's cybersecurity risks (Wang et al. 2013; Kwon and Johnson 2014, 2018; Angst et al. 2017), and therefore, these findings suggest that revealing such investments can reduce the operational risk in the firm. The proven preventive value of cybersecurity investments, on the one hand, and the lack of public information on these cybersecurity investments, on the other hand, make the discretionary disclosure of these investments through proper channels with investors (such as SEC filings) instrumental in reducing information asymmetries about firms' ability to mitigate cybersecurity risks. Hence, we hypothesize that disclosure of cybersecurity investments reduces the premium that investors charge firms for the capital they borrows. Accordingly, we propose the following hypothesis.

Hypothesis 1. *DCI is associated with a lower cost of capital for a firm.*

2.3. Underlying Mechanisms

Disclosures in periodic reports such as 10-K filings tend to be brief and lack granular detail, making them less impactful on their own in directly influencing a firm's cost of capital. However, DCIs can play a significant role as *signals* by attracting the attention of information intermediaries, such as financial analysts, who have the responsibility to interpret and evaluate these signals. As Blankespoor et al. (2020) explain, processing corporate disclosures and information intermediation incurs awareness, acquisition, and integration

costs.[6] Investors may not even notice certain disclosures without intermediaries discussing such information, thus bringing awareness to the disclosures. After noticing the disclosure, although some investors can make judgments on their own, others need help to integrate the new information. Acting as intermediaries between the firm and the market, analysts play a crucial role in shaping investors' perceptions by parsing these disclosures. Although the content of DCIs may seem brief at first glance, they are scrutinized by intermediaries who access proprietary tools and private data sources, enabling a deeper examination of the firm's actual investments and strategic measures. This scrutiny provides a more nuanced understanding of the firm's cybersecurity efforts, and if these efforts are verified to be robust and well executed, the capital market can price in the reduced cyber risk, thus reducing the firm's cost of capital.

As such, not all DCIs are created equal in their capacity to affect the cost of capital. We expect that those DCIs that are less standard—less similar to usual and sometimes boilerplate DCIs that become normatively part of periodic disclosures—are more likely to yield tangible financial benefits. Also, firms that make investments in cybersecurity, supporting the signals sent through DCIs, are more likely to see reduced borrowing costs. This is because such firms can signal to analysts and investors that they are proactively managing risks related to digital security, reducing perceived uncertainties and instilling greater investor confidence. Ultimately, the strength of these signals, amplified through the attention of information intermediaries, can translate into a lower cost of capital for firms that effectively manage their cybersecurity narratives.

2.3.1. Moderating Role of Disclosure Informativeness.

The existing literature already shows that even nuanced aspects of language used in disclosures can be sensed, interpreted, and impounded in price and risk by information intermediaries and investors. For instance, Li (2010) shows that qualitative narratives, such as those found in the Management Discussion and Analysis (MD&A) sections of 10-K filings, carry information that complements financial data and highlights how textual analysis of these disclosures can reveal management's sentiment and how it influences investor behavior.

Particularly, language dissimilarity has been shown to be indicative (or a signal) for more profound differences across firms (or relative to the history of the firm), therefore increasing the "informativeness" of disclosure. Here, informativeness refers to the extent to which a brief disclosure can stand out to catch the attention of information intermediaries. For instance, Hoberg and Phillips (2016) develop a measure of "textual dissimilarity" by comparing 10-K filings across firms and find that firms with more dissimilar disclosures often exhibit distinct business strategies and face unique risks or opportunities that are not shared by industry peers. This dissimilarity is used as a proxy for product differentiation and firm uniqueness. Likewise, Brown and Tucker (2011) analyze changes in the MD&A sections of 10-K filings and show that increased textual dissimilarity across years is associated with the presence of new risks or changes in business strategy. They show that lingual differences signal a firm's distinct response to evolving market conditions or internal changes. Cohen et al. (2020) argue that textual dissimilarity in corporate disclosures often signals important differences in firm risk or strategy. They unravel that markets sometimes overlook these differences, leading to "lazy pricing," where firms with distinct risks or strategies are not appropriately differentiated in their valuations.

In line with past literature, we argue that DCIs that are dissimilar to those made by other firms or from a firm's own previous disclosure can serve as informative signals that catch the attention of information intermediaries. This will then lead to further parsing of information by intermediaries and enhances the impact of DCIs on the cost of capital. Therefore, we hypothesize the following.

Hypothesis 2. *Informativeness of disclosed cybersecurity investments strengthens the negative association between DCI and the cost of capital.*

2.3.2. Moderating Role of Analyst Coverage.

As key information intermediaries, analysts are industry 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 valuation (Barber et al. 2001, Bradshaw et al. 2006). Research has shown that analysts reduce information asymmetries by operating as "information intermediaries" that highlight disclosures that may otherwise have gone unnoticed (Blankespoor et al. 2020) and translate signals sent from firms into insights that are comprehensible by investors and significantly contribute to the returns that a firm earns (Barber et al. 2001, Luo et al. 2015). For instance, Luo et al. (2015) show that analysts play a critical role in helping firms increase their returns by informing investors when firms engage in activities that boost their corporate social responsibility ratings.

Particularly, analysts are shown to be effective in commenting on technological initiatives that firms undertake. For instance, the existing literature (Benner 2010) has shown that analysts are effective in applying institutional pressures on firms they cover to make them conform to new technological practices, especially in the case of disruptive technological changes. That said, not all firms are covered equally by financial

analysts. Firms with more coverage benefit from a lower information asymmetry. These analysts can engage in additional due diligence by leveraging proprietary data (Chi et al. 2024) that further verify the fundamental value of these signals. Such due diligence include accessing private reports about the firm's actual cybersecurity investments, as well as the subsequent vulnerability test results that are often not public but can be accessed upon request of analysts. As such, we expect that if an observed negative association between DCI and the cost of capital is due to reduced information asymmetries happening through information intermediation, that association should be strengthened for firms with more informational intermediaries (more analysts following the firm). Accordingly, we propose the following hypothesis.

Hypothesis 3. *Analyst coverage of a firm strengthens the negative association between DCI and the cost of capital.*

3. Empirical Design

3.1. Data and Sample

In creating our sample, we followed Gordon et al. (2010) and obtained 10-K disclosures of public firms from 2006 to 2018. The sample starts from 2006 when the SEC started to publicly share CL reviews, which we use as an instrumental variable (see Section 3.3). A firm is retained in the sample only if all its financial information, industry classification, and the values of the other variables in our empirical estimation (discussed below) are available. To ensure comparability in debt markets, our data exclude foreign firms, including those listed in the United States as common stock or American Depositary Receipts. Using the industry identifications of Fama and French (1997), we further eliminate firms in banking, insurance, and real estate,[7] given that their capital structures are highly regulated and vastly different from other industries. Prior studies related to capital and debt raising have similarly excluded these firms from the main sample (Billett and Xue 2007, Bates et al. 2009, Kisgen 2009). We exclude firm-year observations not included in Aberdeen's Computer Intelligence Technology Database (CITDB)[8] and winsorize the data at each 1% tail, following Frank and Shen (2016). This results in a sample of 16,680 firm-year observations of 1,933 firms from 2006 to 2018.[9] The sample firms primarily operate in manufacturing, information, retail, wholesale trading, utilities, transportation and warehousing, and healthcare.

3.1.1. Measuring the Disclosure of Cybersecurity Investments. Following Gordon et al. (2010), we measure a firm's DCI in year t by considering whether the firm made such disclosure in their SEC report during that year (zero/one dummy).[10] The 10-K reports for the observations in the sample are collected from the SEC's Electronic Data Gathering, Analysis, and Retrieval (EDGAR) system. The collected 10-Ks were obtained in HTML format, and the content of each div and p tag was then transferred to a CSV file (as separate documents in a 10-K corpus) for feature extraction. The regular text cleaning approaches, including turning to lower cases, lemmatizing, and removal of stop words, were done for all documents in the 10-K corpus.

Paragraphs containing a set of some general keywords pertaining to cybersecurity (listed in Online Appendix C) are automatically highlighted by a search algorithm, and reports with at least one hit are then manually inspected by two research assistants. During this process, observations irrelevant to a cybersecurity announcement and those pertaining to cybersecurity but irrelevant to a cybersecurity investment (e.g., a statement pertaining to cybersecurity risks the firm faces but not to the investments it makes) are also marked. Of the 1,933 sample firms, 814 firms (almost 42%) have at least one report with a confirmed DCI.

3.1.2. Cost of Capital. Following existing literature (Sharfman and Fernando 2008, Dhaliwal et al. 2011), the main outcome variable, cost of capital (COC), is expressed as the firm's after-tax weighted average cost of capital:

$$\text{COC} = \left(\frac{E}{E+D}\right) r_E + \left(\frac{D}{E+D}\right) r_D(1-T),$$

where r_E is the firm's cost of equity (COE) capital, r_D is the firm's cost of debt (COD) capital (retrieved from Bloomberg Financial),[11] and T is the firm's rate of corporate taxation. E and D are the market values of the firm's equity and debt, respectively. The notation r_E denotes the expected return from holding the firm's equity (cost of 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 U.S. treasury bond rate), r_M is the return on the market portfolio, and β_E is the firm's systematic risk $\frac{Cov(r_M, r_F)}{Var(r_M)}$. In the main analysis, the cost of capital is estimated for a period of 30 days starting from the date of disclosure of the 10-K report by the firm. This 30-day period starts from the date of disclosure of the 10-K report by the firm. This postdisclosure period is a major point of the year for markets and investors to react to the most comprehensive and influential periodic report that public firms release. The measure captures these reactions through stock and bond price variations.

3.1.3. Informativeness and Coverage. To assess the *informativeness* of cybersecurity investment disclosures,

we adopt a cosine similarity measure, following Brown and Tucker (2011) and Cohen et al. (2020). The measure is calculated as one minus the cosine similarity between a firm's DCI and that of its industry benchmarks. The intuition for the measure is that the more distinct a DCI is from its benchmark disclosures, the more informative it is. To estimate the cosine similarity between a firm's disclosures of cybersecurity investments and those of its benchmarks, the stop words in the corpora of the focal firm and its benchmark are first removed, and all words are lemmatized. In each corpus, the weight of each word is assigned using term frequency–inverse document frequency (TF-IDF), which assigns a weight to each word based on how commonly used the word is and how frequently it is used in the document. The vectors of words in the corpus of the focal firm are then compared with the vector of words in the corpus of each benchmark, and one minus the average of the cosine similarity scores of the focal firm and its benchmarks is used as a measure of informativeness. For the main measure of informativeness, the industry benchmark includes peer firms in the same year and in the same four-digit Standard Industry Classification (SIC) code. We also test for alternative measures of informativeness using other benchmarks in the cosine similarity measure.

Following the existing literature (Bhushan 1989, He and Tian 2013), 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 Institutional Brokers' Estimate System (IBES) database. We expect that with more financial analysts covering a firm, its disclosure on cybersecurity investments will be better understood by the capital market. In a subsequent test, we also test for coverage by analysts with domain knowledge in cybersecurity.

3.1.4. Information Technology Expenditure. Because firms' information technology (IT) infrastructure has a key effect in regulating cyber risks (Li et al. 2023), we control for *IT expenditure* in the specification. *IT expenditure* is measured by the deflated value of IT stock for each firm from CITDB[12] and then divided by the deflated value of annual sales (Saunders and Brynjolfsson 2016, Nagle 2019). Following the existing literature, the value of IT stock is estimated by summing the value of IT hardware and three times the value of IT labor. The market value of IT hardware is estimated by multiplying the number of PCs and servers that a firm has by the average price of the PC/server extracted from the Telecommunications database of the Economist Intelligence Unit (Nagle 2019). The price indices for nonresidential computers and peripherals provided by the Bureau of Economic Analysis (BEA) are then used to deflate the value of IT hardware.

The value of IT labor is estimated by multiplying the number of IT workers in each firm (provided by CITDB) and the average annual wage for computer and mathematical science occupations, sourced from the Bureau of Labor Statistics. The Employment Cost Index for Wages and Salaries of management, professional, and related occupations at the industry level are used to deflate the value of IT labor. The deflated value of IT stock (deflated value of IT hardware + deflated value of IT labor) is then divided by annual sales, which itself is deflated by BEA's gross domestic product (GDP) Price Index for gross output to measure IT expenditure.

3.1.5. General Disclosure Quality. We control *general disclosure quality* in the specification because the main instrumental variable may shift the overall disclosures beyond DCI, which could affect the estimate of the main effect. *General disclosure quality* is measured following Chen et al. (2015), who count nonmissing data items in the firm's 10-K reports as reported in COMPUSTAT. Particularly, the approach is based on disclosure quality values in the balance sheet and income statement. To measure the disclosure quality of the balance sheet, we rely on Chen et al.'s hierarchy of groups (11), parent accounts (25), and subaccounts (93). We count the number of nonmissing items in the subaccounts of a given group and divide that by the total number of subaccounts of that group. This ratio is then multiplied by a weight (the sum of assets in that balance sheet item group/the value of assets), summed for all 11 groups, and divided by 2, to create a balance-sheet disclosure quality that varies between 0 and 1. Similarly, for the income statement, Chen et al. (2015) define seven groups of accounts that link with 51 subaccounts. An equal-weight average[13] of nonmissing item ratios across the seven groups of income statements makes up the disclosure quality of the income statement. The average value of disclosure quality of the balance sheet and the income statement is then used as a proxy for the overall disclosure quality (Chen et al. 2015).

3.1.6. Other Controls. We control for a rich set of firm-level variables that are frequently used as time-varying covariates when estimating business profitability and costs in conjunction with digital investments (Bardhan et al. 2013, Mithas et al. 2017, Havakhor et al. 2019). In particular, *diversification* is evaluated by the entropy measure (Robins and Wiersema 1995). It is calculated using the difference between total and unrelated diversification, which in turn depends on percentages of sales across different industries. We measure firm *size* as the natural log of the number of employees in thousands. Total *assets* (in millions of dollars) are measured using reported data from COMPUSTAT and following

Nagle (2019).[14] *R&D* and *advertising expenditures* are estimated using the deflated value of investments in R&D and advertising divided by the deflated value of the firm's annual sales.[15]

Because several general noncybersecurity factors can determine a firm's cost of capital, it is imperative to isolate the effect of those factors, especially if they are time varying. Accordingly, we include several additional controls that the literature (Sharfman and Fernando 2008, Luo et al. 2015) 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 recommendations. Further, we include *analysts' exposure* (firm-specific experience ln(1 + average number of years the firm was covered by analysts)) (Chen and Matsumoto 2006), which enhances the quality of analysts as information intermediaries. Both forecast error and analysts' exposure adjust for the possible biases in analyst coverage a firm receives.

We also control for the number of *corporate social responsibility* (*CSR*) *disclosures* (the number of public disclosures about a firm's socially responsible activities as reported in the CSR newswire and Corporateregister.com) because CSR disclosures are known to reduce the cost of capital (Dhaliwal et al. 2011) and are associated with cyber risks (D'Arcy et al. 2020). The inclusion of this variable is important because a firm may have engaged in several activities to lower its noncybersecurity risk, and without accounting for these other risk-reducing activities, the impact of the DCI on the cost of capital cannot be assessed. Similarly, we follow Merkley (2014) and control for the number of *noncybersecurity disclosures* (ln(number of non–cybersecurity-related sentences in the SEC reports)), as another indicator of the disclosure of other activities related to general firm risks.

Panel A of Table 1 presents the correlation matrix, and panel B presents descriptive statistics for the key variables across the entire sample as well as by treated versus untreated firms. Specifically, the last column in panel B reports the *t*-statistics comparing the means for firms with DCI always equal to zero (1,119 firms) and firms that have at least one observation with DCI greater than zero (814 firms). First, the two types of firms are different in their average COC, with firms showing at least one DCI having a lower COC. These comparisons also reveal that firms with no DCI have a larger employee base and asset size but show moderately lower amounts of R&D expenditure. 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, noncybersecurity disclosure, and general disclosure quality. This implies that the significant difference in COC between the two groups may not be explained sufficiently by known factors contributing to COC. This provides some model-free evidence of the importance of considering DCI in explaining cross-firm differences in terms of COC.

3.2. Main Specification

To formally test our hypotheses, the main empirical estimation is specified as follows:

$$\begin{aligned} Outcome_{it} &= \beta \cdot DCI_{it} + \xi \cdot Coverage_{it} + \lambda \cdot Informativeness_{it} \\ &\quad + \phi \cdot Coverage_{it} \times \mathrm{DCI}_{it} + \eta \cdot Informativeness_{it} \times DCI_{it} \\ &\quad + \gamma \cdot Control_{it} + INDUSTRY\_YEAR + FIRM_i + \epsilon_{it}, \end{aligned} \quad (1)$$

where *DCI* is the zero/one dummy representing disclosure of cybersecurity investments, subscripts *i* and *t* denote firm *i* in year *t*, and ϵ_{it} is the error term. *Control* is the set of control variables outlined above. $FIRM_i$ is firm fixed effects, and *INDUSTRY_YEAR* represents the industry-year fixed effect dummies. We use the combined fixed effects to account for macro events that may affect different industries differently. To test the underlying mechanism (Hypotheses 2 and 3), the informativeness of disclosures (*Informativeness*), the extent of analyst coverage (*Coverage*), and their interactions with *DCI* are included in the specification after we test the main effect without the moderators. The main outcome variable is the cost of capital. Additionally, we test the model on the cost of equity and cost of debt to assess its impact on the equity and debt markets independently.

3.3. Identification Strategy

Identifying the impact of DCI on the cost of capital in field settings presents several challenges, which our empirical approach is specifically designed to address. First, cybersecurity investments operate in tandem with other IT investments that a firm makes, and existing research shows that IT investments by a firm can reduce information uncertainty about the firm (Jia et al. 2020). Therefore, IT expenditure can systematically influence both investments in cybersecurity and, subsequently, their disclosure and the firm's cost of capital. Hence, any empirical approach to constructing an observational sample should incorporate a reasonably accurate estimate of IT expenditure as an explanatory variable when modeling variation in the cost of capital. Consequently, we construct our sample by focusing on firms whose IT expenditures are profiled and accessible to capital markets. Although IT rankings, such as those made by InformationWeek,

Table 1. Correlations and Summary Statistics

Panel A: Correlation matrix

	Variable	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	*DCI*																
2	*Informativeness*	**0.204**															
3	*Coverage*	**−0.061**	−0.014														
4	*COC*	**−0.212**	**−0.153**	**0.039**													
5	*COE*	**−0.258**	**−0.201**	0.008	**0.885**												
6	*COD*	**−0.314**	**−0.185**	**0.018**	**0.785**	**0.514**											
7	*IT Expenditure*	**0.098**	**−0.021**	**0.039**	**−0.031**	**−0.066**	**−0.053**										
8	*Firm Size*	**−0.028**	0.013	**0.093**	**0.061**	**0.058**	**0.045**	**0.186**									
9	*Assets*	**−0.133**	0.004	**0.097**	**0.041**	**0.038**	**0.027**	**0.139**	**0.243**								
10	*R&D*	**0.152**	**0.042**	**0.155**	**−0.101**	**−0.089**	**−0.115**	**0.165**	**0.316**	**0.071**							
11	*Advertising Expenditure*	**0.059**	**−0.056**	**0.178**	0.010	0.005	0.008	**0.182**	**0.222**	**0.107**	**0.031**						
12	*Forecast Error*	**0.021**	**−0.078**	**−0.029**	**0.030**	0.002	0.012	**0.050**	**−0.078**	**−0.072**	**0.243**	**0.029**					
13	*Analysts' Exposure*	0.011	**0.033**	**0.049**	**−0.112**	**−0.127**	**−0.145**	**0.029**	**0.082**	**0.078**	**0.108**	**0.137**	**−0.124**				
14	*CSR*	**0.075**	**−0.072**	**−0.041**	**0.188**	**0.231**	**0.315**	**0.020**	**0.139**	**0.081**	**−0.091**	**0.204**	**0.049**	**0.081**			
15	*Noncyber Disclosure*	**−0.033**	**0.119**	**0.052**	**−0.041**	**−0.038**	**−0.058**	**−0.061**	**0.272**	**0.235**	**−0.118**	**0.109**	**−0.061**	**0.068**	**−0.059**		
16	*General Disclosure Quality*	**0.111**	**0.241**	−0.010	**−0.216**	**−0.189**	**−0.236**	**−0.081**	**0.172**	**0.178**	**−0.082**	**0.143**	**−0.091**	**0.068**	**−0.153**	**0.082**	
17	*Diversification*	**0.208**	−0.004	−0.011	**−0.017**	**−0.086**	**−0.088**	**−0.092**	**0.113**	**0.118**	**−0.064**	**0.126**	**−0.073**	**0.044**	0.007	**0.093**	**0.188**

Panel B: Summary statistics and univariate comparisons

		Full sample (N = 16,680)					DCI = 0 (N_0 = 1,119)		DCI = 1 (N_1 = 814)		
	Variable	Mean	Standard deviation	Median	Minimum	Maximum	Mean	Standard deviation	Mean	Standard deviation	*t*-diff
1	*DCI*	0.216	0.412	0	0	1	—	—	—	—	—
2	*Informativeness*	0.171	0.262	0.122	0.003	1	—	—	—	—	—
3	*Coverage*	1.021	0.883	1.099	0	2.079	1.022	0.947	1.011	0.865	0.261
4	*COC*	0.085	0.065	0.084	0.065	0.118	0.092	0.062	0.085	0.064	2.418***
5	*COE*	0.098	0.052	0.089	0.026	0.211	0.105	0.048	0.082	0.054	9.865***
6	*COD*	0.044	0.023	0.046	0.008	0.098	0.052	0.021	0.038	0.027	12.817***
7	*IT Expenditure*	0.031	0.038	0.04	0.012	0.092	0.030	0.045	0.032	0.032	−1.085
8	*Firm Size (in thousands)*	21.328	3.099	17.602	2.008	132.954	18.357	3.099	17.814	3.168	3.771***
9	*Assets (in millions)*	1,298.545	8.602	6,747.99	71.665	61,389.863	1,319.489	8.440	1,052.58	18.973	416.715***
10	*R&D*	0.082	0.165	0.068	0	0.64	0.072	0.154	0.085	0.274	−1.324
11	*Advertising Expenditure*	0.028	0.116	0.030	0	0.155	0.028	0.123	0.029	0.123	−0.177
12	*Forecast Error*	0.031	0.213	0.412	0.008	0.275	0.029	0.22	0.03	0.21	−0.101
13	*Analysts' Exposure*	1.463	0.989	1.329	0.697	2.121	1.428	1.049	1.483	0.98	−1.172
14	*CSR*	0.020	0.141	0	0	1	0.020	0.138	0.021	0.135	−0.159
15	*Noncyber Disclosure*	7.997	1.778	7.085	6.791	8.712	7.914	3.741	8.021	1.656	−0.768
16	*General Disclosure Quality*	0.714	0.224	0.752	0.412	0.921	0.774	0.198	0.785	0.239	−1.105
17	*Diversification*	0.161	0.341	0.178	0.012	0.562	0.162	0.158	0.169	0.244	0.764

Notes. Panel A of this table presents the correlations between all variables in the main analyses. Correlation coefficients significant at the 5% level are bold. *COC* stands for the cost of capital, which is a weighted average of the cost of equity and the cost of debt. *DCI* stands for disclosure of cybersecurity investments, which equals one if firms disclose at least one cybersecurity investment in their SEC filings in the current year and zero otherwise. *Coverage* is the number of financial analysts covering the firm. *Informativeness* equals one minus the cosine similarity of DCI between the focal firm and its peer firms in the same four-digit SIC code. See Online Appendix B for all variable definitions. Panel B presents summary statistics and univariate comparisons between firms with at least one disclosure of cybersecurity investments and firms with no disclosure. Statistics for informativeness are for the treated group only, as it is set at zero for the control group. N_0, N_1 are the number of firms in the respective subsamples. Summary statistics are based on firm-year observations (N).

*** stands for statistical significance at 1%.

are a proper source, they cover a limited set of IT-investing firms. By contrast, market intelligence databases, most notably CITDB, cover a broader range of IT-investing firms and are available to capital markets.[16] In addition to IT expenditure, extensive research has identified a host of factors that can influence the cost of capital. Although the connections between these factors and DCI are less apparent than those between IT expenditure and DCI, our econometric models include a reasonable set of these factors.

Second, because DCI falls under managerial discretion, the incidence of DCI by a firm is not randomly determined and is potentially endogenous. Our identification strategy relies on two well-established approaches to address this endogeneity concern. First, and given that our sample spans a rather extensive period of time, from 2006 to 2018, we account for firm fixed effects; this ensures that the time-invariant omitted variables are absorbed. Second, we use an instrumental variables approach. To do so, we searched for relevant reasonably exogenous shocks (i.e., exogenous to managerial discretion) that could impact DCI while ensuring that they met the exclusion criteria. Note that excluding the shock itself from the second stage of the two-stage least squares (2SLS) does not introduce misspecification bias.

The issuance of a CL by the SEC satisfies the criteria of a valid instrument. Section 408 of the Sarbanes–Oxley Act (2002) lays out several factors that trigger SEC reviews, and disclosure of cybersecurity investments is not one of them.[17] Specifically, a CL is a dialogue between the SEC and a firm about its disclosures. Section 408 of the Sarbanes–Oxley Act of 2002 requires the SEC to review U.S. listed firm filings at least once every three years. Similar to the Internal Revenue Service's audit formula, the SEC does not discuss the specifics of when and why certain firms are reviewed. If the SEC deems that there is a potential problem that needs clarification, a CL is issued. Roughly 20%–40% of companies receive CLs each year (Heese et al. 2017).[18] Most CLs do not result in refilings of 10-Ks. When the issue is clarified, firms receive a "no further comment" letter.

CLs are issued by the SEC as part of the "review of disclosure filings," such as those from the previous years, 8-Ks, and 4Qs. Notably, before disseminating CL reviews on EDGAR, the public is unaware of the reviews.[19] In August 2004, the SEC decided to release all completed reviews to the public no later than 45 days after the completion of the review,[20] and in January 2012, it reduced that period to 20 business days.[21]

Although CL reviews are not triggered by DCI, firms are required to disclose material information to stakeholders, and activities pertinent to cybersecurity are particularly mandated by the SEC.[22] The SEC's guidance states:

> Although no existing disclosure requirement explicitly refers to cybersecurity risks and cyber incidents, a number of disclosure requirements may impose an obligation on registrants to disclose such risks and incidents. In addition, material information regarding cybersecurity risks and cyber incidents is required to be disclosed when necessary in order to make other required disclosures, in light of the circumstances under which they are made, not misleading.

When a review is pending, alerted firms are motivated to disclose more material information in public disclosures (Duro et al. 2019). Therefore, under SEC scrutiny, firms are motivated to voluntarily disclose various information, including information about cybersecurity investments, as a signal of lower cybersecurity risk (i.e., the CL review meets the *relevance* requirement for instrumental variables).

Given that CL reviews are published only upon completion, there is a period during which managers are motivated to improve the quality of their disclosures, but capital markets are still not privy to the review in progress (hereafter, the private review phase). This ensures that the CL review meets the *conditional exogeneity* requirement for instrumental variables. Therefore, our models are instrumented using *CL_Review*, which equals one if the firm has a CL review issued before a firm discloses its 10-K reports and equals zero otherwise. The private review phase extends to the period in which we estimate the cost of capital (COC) (a 30-day window after the disclosure of the 10-K report). As a result, this instrument helps to achieve a conditional random assignment of the treatment variable: DCI.

Note that CL reviews may motivate improvements in other aspects of the disclosure as well. Therefore, to meet exclusion criteria and ensure unbiased estimates in the 2SLS specification, we include a measure of *general disclosure quality* (for sections of the 10-K other than those related to DCI) as an additional covariate in the 2SLS specifications. Beyond enhancing disclosure quality and increase the likelihood of DCI, CL reviews cannot directly influence the COC because, during the period in which the COC is estimated, the review remains private and unknown to capital markets. This ensures the conditional exogeneity needed for identification, and the exclusion of the instrument from the second stage will not result in an omitted variable bias. In a times-to-event model (COX regression), we find that known covariates cannot predict CL_Review (Table E.2, Online Appendix E), which further ensures exogeneity.

Because *DCI* is a binary variable, we follow the existing literature (Angrist and Pischke 2009, Chen et al. 2021) by first estimating a probit model with *DCI* as the outcome variable and *CL_Review* as the instrument while including the remaining covariates. The

predicted value from this probit model (denoted by $\widehat{DCI}$) is then used as the instrument in the 2SLS procedure. The predicted instrument shows strong statistical relevance to the endogenous variables (see the stage 1 estimations in Table E.3 in Online Appendix E). To increase the interpretability of the coefficient estimates, all continuous variables are standardized. To ensure the external validity of the 2SLS, we compare firm characteristics for observations with small and large residuals in stage one (Bennedsen et al. 2007, Roberts and Whited 2013) and find largely nonsignificant differences (Table E.4 in Online Appendix E), suggesting that observations strongly affected by the instrument are ex ante similar to those less affected.

4. Results

Before discussing the findings in detail, we outline the main and additional analyses. The main analyses utilize a 2SLS with a fixed effects model to test how DCI affects COC (Section 4.1). We verify the underlying mechanism by testing interactions between DCI and the informativeness of disclosure (Section 4.1), analyst coverage (Section 4.1), cybersecurity investments (Section 4.2.1), and institutional holdings (Section 4.2.2). To examine the robustness of the identification, we use three alternative instruments for DCI (Section 5.1) and instrument analyst coverage (Section 5.2). We also conduct placebo and falsification tests to rule out alternative explanations for our findings (Section 5.3). Further, we test the effect of first-time DCI under a DID framework (Section 6.1) and conduct subsample analyses for periods when firms raise capital (Section 6.2).[23]

4.1. Main Findings

We conduct our main analyses using a panel 2SLS fixed effects regression.[24] We first conduct univariate analyses testing the relationships between DCI and COC, COE, and COD (Table 2, panel A, columns 1–3, respectively), and find a positive effect of disclosing cybersecurity investments on reducing COC and both of its components: COE and COD. Next, we include firm fixed effects while excluding control variables (Table 2, panel A, columns 4–6). We then estimate Equation (1) with the full set of control variables. Consistent with columns 1 and 4, column 7 of Table 2, panel A, shows that DCI significantly reduces the cost of capital (supporting Hypothesis 1). Additionally, when the cost of equity (COE) and the cost of debt (COD) replace COC as the outcome variable, the results remain qualitatively unchanged. The effect size from column 1 suggests that an average firm disclosing cybersecurity investments access capital at a rate 7.6% lower than that of its nondisclosing counterparts.[25]

In Table 2, panel B, we estimate Equation (1), including the interaction terms. The main effect of DCI on COC persists after including the moderation terms.[26] The negative and significant coefficients of both coverage×DCI and informativeness×DCI provide support for Hypothesis 2 and Hypothesis 3, suggesting that the impact of DCI on the cost of capital is impacted by how granular the information communicated in DCI is and how well bridged a firm is to its investors for them to parse signals sent through DCI.[27] Because cybersecurity risks have generally increased in recent years and the SEC has also released mandates demanding more clarity related to these increased risks, we further examine whether more recent DCIs have a stronger effect on COC by the linear time trend (t) as a moderator for DCI. We find that DCIs in more recent years have a stronger effect on COC (Table 2, panel B, columns 10–12), suggesting that cybersecurity is becoming an increasingly important factor in capital markets.

4.2. Further Analyzing the Underlying Mechanism

Broadly speaking, Hypothesis 2 and Hypothesis 3 clarify the boundary conditions underlying the DCIs' impact on COC; particularly (1) the information in DCIs that can help lenders and investors calibrate their assessment of risk and (2) the information intermediaries that can help to parse signals sent through DCIs. The sections below dive deeper into the two mechanisms. In sum, we explain that gauging the actual investments in cybersecurity also helps signal lenders and investors for better risk calibration, whereas the degree of institutional ownership is an alternative way of understanding how effectively the signals sent through DCIs can be parsed.

4.2.1. Accounting for the Effect of Investment in Cybersecurity. Our theoretical argument rests on a signaling mechanism whereby DCI operates as a signal that invites investors' scrutiny of a firm's cybersecurity investments, leading to a reduction in information asymmetry, a better assessment of risk, and thereby a reduction in COC. If this causal path is valid, we should not see a significant impact of DCI on COC in cases where the firm does not sufficiently invest in cybersecurity. Alternatively, a firm investing sufficiently in cybersecurity but not disclose those investments in its public reports should not experience a significant reduction in COC either. In other words, the COC of such a firm should be comparable to the COC of a firm without sufficient investments and no disclosure of DCI. To see whether this is indeed the case, we need to quantify the extent of a firm's investment in cybersecurity. To this end, we utilize the new data set that the Aberdeen Group maintains along with the CITDB, which has been available from 2010 onward, to

Table 2. Main Analyses

Panel A: Main analyses without moderators

Variable	*COC* (1)	*COE* (2)	*COD* (3)	*COC* (4)	*COE* (5)	*COD* (6)	*COC* (7)	*COE* (8)	*COD* (9)
DCI	−0.099***	−0.092***	−0.088***	−0.108***	−0.105***	−0.081***	−0.079***	−0.073**	−0.072**
	(0.009)	(0.014)	(0.017)	(0.012)	(0.012)	(0.015)	(0.012)	(0.042)	(0.037)
Firm Size							0.002**	0.002**	0.002**
							(0.001)	(0.001)	(0.001)
Assets							0.009	0.005*	0.006
							(0.006)	(0.003)	(0.004)
Diversification							0.001	0.001	0.001
							(0.001)	(0.001)	(0.001)
R&D							−0.124***	−0.145***	−0.179***
							(0.027)	(0.029)	(0.031)
Advertising Expenditure							0.003	0.689***	1.768***
							(0.002)	(0.236)	(0.349)
IT Expenditure							−0.038	−0.047*	−0.047*
							(0.032)	(0.026)	(0.025)
Forecast Error							0.003	0.003	0.004
							(0.003)	(0.002)	(0.003)
Analysts' Exposure							0.012*	0.012	0.012
							(0.007)	(0.008)	(0.01)
CSR							−0.196***	−0.140***	−0.102***
							(0.035)	(0.021)	(0.024)
Noncyber Disclosure							−0.008	−0.008	−0.009
							(0.005)	(0.005)	(0.007)
General Disclosure Quality							−0.076**	−0.094**	−0.077***
							(0.035)	(0.046)	(0.029)
Wald's chi	1,205	1,782	1,333	3,487	3,878	3,269	12,145	12,146	18,451
Firm fixed effects	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes
Year-industry fixed effects	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
No. of firms	1,933	1,933	1,933	1,874	1,874	1,874	1,874	1,874	1,874
Observations	16,680	16,680	16,680	16,621	16,621	16,621	16,621	16,621	16,621

Panel B: Main analyses with moderators

Variable	*COC* (1)	*COE* (2)	*COD* (3)	*COC* (4)	*COE* (5)	*COD* (6)	*COC* (7)	*COE* (8)	*COD* (9)	*COC* (10)	*COE* (11)	*COD* (12)
DCI	−0.102***	−0.092**	−0.079**	−0.102***	−0.097**	−0.079**	−0.097***	−0.095**	−0.081**	−0.041***	−0.039***	−0.042***
	(0.022)	(0.045)	(0.035)	(0.022)	(0.043)	(0.037)	(0.022)	(0.043)	(0.036)	(0.011)	(0.008)	(0.007)
Informativeness	−0.006	−0.007	−0.006				−0.006	−0.007	−0.006			
	(0.005)	(0.006)	(0.005)				(0.005)	(0.006)	(0.005)			
Informativeness × DCI	−0.062*	−0.052**	−0.064**				−0.061*	−0.051*	−0.067**			
	(0.036)	(0.026)	(0.026)				(0.034)	(0.027)	(0.027)			
Coverage				−0.011	−0.014	−0.014	−0.011	−0.014	−0.014			
				(0.008)	(0.009)	(0.011)	(0.008)	(0.009)	(0.011)			

Table 2. (Continued)

Panel B: Main analyses with moderators												
Variable	*COC* (1)	*COE* (2)	*COD* (3)	*COC* (4)	*COE* (5)	*COD* (6)	*COC* (7)	*COE* (8)	*COD* (9)	*COC* (10)	*COE* (11)	*COD* (12)
Coverage × *DCI*				−0.081**	−0.047	−0.079*	−0.085**	−0.048*	−0.082**			
				(0.039)	(0.029)	(0.043)	(0.04)	(0.028)	(0.041)			
t										−0.121***	−0.014***	−0.112***
										(0.022)	(0.021)	(0.017)
t × *DCI*										−0.082***	−0.056***	−0.093***
										(0.012)	(0.008)	(0.018)
Firm Size	0.002**	0.002**	0.002**	0.002**	0.002**	0.002**	0.002	0.002	0.002	0.002**	0.002**	0.002**
	(0.001)	(0.001)	(0.001)	(0.001)	(0.001)	(0.001)	(0.001)	(0.001)	(0.001)	(0.001)	(0.001)	(0.001)
Assets	0.009	0.005*	0.006	0.009	0.005*	0.006	0.009	0.005	0.006	0.009	0.005*	0.006
	(0.006)	(0.003)	(0.004)	(0.006)	(0.003)	(0.004)	(0.006)	(0.003)	(0.004)	(0.006)	(0.003)	(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)	(0.001)	(0.001)	(0.001)	(0.001)	(0.001)	(0.001)	(0.001)	(0.001)	(0.001)	(0.001)
R&D	−0.117***	−0.135***	−0.174***	−0.129***	−0.136***	−0.183***	−0.123***	−0.142***	−0.181***	−0.128***	−0.139***	−0.179***
	(0.026)	(0.03)	(0.03)	(0.026)	(0.028)	(0.029)	(0.027)	(0.029)	(0.031)	(0.026)	(0.028)	(0.032)
Advertising Expenditure	0.003	0.724***	1.733***	0.003	0.675***	1.715***	0.003	0.703***	1.75***	0.003	0.717***	1.68***
	(0.002)	(0.24)	(0.339)	(0.002)	(0.219)	(0.36)	(0.002)	(0.231)	(0.346)	(0.002)	(0.226)	(0.339)
IT Expenditure	−0.038	−0.05*	−0.047*	−0.039	−0.049**	−0.046*	−0.038	−0.048*	−0.047*	−0.04	−0.048*	−0.046*
	(0.032)	(0.026)	(0.026)	(0.031)	(0.024)	(0.027)	(0.032)	(0.025)	(0.026)	(0.034)	(0.026)	(0.025)
Forecast Error	0.003	0.003	0.004	0.003	0.003	0.004	0.003	0.003	0.004	0.003	0.003	0.004
	(0.003)	(0.002)	(0.003)	(0.003)	(0.002)	(0.003)	(0.003)	(0.002)	(0.003)	(0.003)	(0.002)	(0.003)
Analysts' Exposure	0.012*	0.011	0.012	0.012*	0.012	0.012	0.012	0.012	0.012	0.012*	0.012	0.013
	(0.007)	(0.008)	(0.01)	(0.007)	(0.008)	(0.01)	(0.007)	(0.008)	(0.01)	(0.007)	(0.008)	(0.01)
CSR	−0.194***	−0.135***	−0.103***	−0.19***	−0.136***	−0.096***	−0.192***	−0.139***	−0.101***	−0.184***	−0.14***	−0.105***
	(0.034)	(0.02)	(0.023)	(0.032)	(0.022)	(0.025)	(0.034)	(0.021)	(0.024)	(0.035)	(0.02)	(0.023)
Noncyber Disclosure	−0.008	−0.008	−0.009	−0.008	−0.008	−0.009	−0.008	−0.008	−0.009	−0.008	−0.008	−0.009
	(0.005)	(0.005)	(0.007)	(0.005)	(0.005)	(0.007)	(0.005)	(0.005)	(0.007)	(0.005)	(0.005)	(0.007)
General Disclosure Quality	−0.081**	−0.092**	−0.074**	−0.081**	−0.089**	−0.076**	−0.077**	−0.093**	−0.075**	−0.076**	−0.097**	−0.071**
	(0.034)	(0.045)	(0.03)	(0.034)	(0.045)	(0.03)	(0.035)	(0.047)	(0.029)	(0.035)	(0.045)	(0.029)
Wald's chi	14,457	15,227	16,459	18,613	17,692	12,308	15,616	15,417	8,969	13,078	17,541	18,927
Firm fixed effects	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Year-industry fixed effects	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
No. of firms	1,874	1,874	1,874	1,874	1,874	1,874	1,874	1,874	1,874	1,874	1,874	1,874
Observations	16,621	16,621	16,621	16,621	16,621	16,621	16,621	16,621	16,621	16,621	16,621	16,621

Notes. This table presents the main regression results. The dependent variables are *cost of capital* (*COC*), *cost of equity* (*COE*), and *cost of debt* (*COD*). *COC* is a weighted average of COE and COD. The independent variable is *disclosure of cybersecurity investments* (*DCI*), which equals one if firms disclose at least one cybersecurity investment in their SEC filings in the current year and zero otherwise. Panel A reports results without moderators. Panel B includes informativeness and coverage as moderators. *Coverage* is the number of financial analysts covering the firm. *Informativeness* equals 1 minus the cosine similarity of DCI between the focal firm and its peer firms in the same four-digit SIC code. See Online Appendix B for detailed variable definitions. All analyses are instrumented using *comment letter review*. All continuous variables are standardized. Standard errors are in parentheses.

***, **, and *Statistical significance at the 1%, 5%, and 10% level, respectively.

control for the impact of the presence of 14 types of cybersecurity-related software and technologies.[28] Specifically, we identified the presence of antivirus 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, and cloud computing. Given that the installation of these software elements is reported at the establishment level of a firm, cybersecurity investment is measured as the ratio of the total number of cybersecurity technologies installed across establishments to the total number of establishments surveyed in that year, across the 14 aforementioned cybersecurity-related software types.

With the measure of cybersecurity investment constructed, we then conduct a moderation test on analyst coverage by interacting cybersecurity investments with DCI. Column 1 of Table 3 shows that the cost of capital is reduced when firms disclose cybersecurity investments (consistent with the main result in Table 2), but the effect of cybersecurity investment itself is insignificant, suggesting that, absent disclosure, a firm may not reap cost-reduction benefits from such investments. Moreover, the effect of disclosures is strengthened when the cybersecurity investment level is higher. This means that the capital market rewards firms that can substantiate their disclosures with actual investments. We observed comparable results for the cost of equity and the cost of debt (columns 2 and 3 of Table 3, respectively).

4.2.2. Institutional Holdings. The moderation test on analyst coverage has revealed its role in strengthening the impact of DCI on COC, which is consistent with an information asymmetry reduction mechanism underlying the DCI→COC link. Although analysts play a key role in discovering, selecting, and interpreting information pertinent to risk, research has suggested that institutional investors are also efficient in interpreting, selecting, and discovering risk-relevant information (Akins et al. 2012). Therefore, if the information conveyed through DCI leads to a reduction in COC, the impact of DCI should also be stronger for firms with a higher level of institutional holdings. Using information from 13-f filings in the last quarter of each year, retrieved from Thomson Reuters, we assess the extent of the institutional holdings (IH) of each firm as the ratio of outstanding shares owned by institutional investors (Chen et al. 2020). IH equals one if a firm has above-median institutional holdings and equals zero otherwise. We include IH and IH×DCI as additional covariates in Equation (1). Results presented in columns 4–6 of Table 3 show that IH×DCI is negative and significant, with COC, COE, and COD as outcome variables. This further shows that DCI serves as a source of risk-reducing signals to capital markets because the impact of DCI is stronger for firms whose investors are better equipped by proxy (i.e., through analysts) or independently (i.e., as institutional investors) to discover, select, and interpret relevant signals.

5. Robustness Checks

5.1. Alternative Instrumentation of DCI

Although CLs are an exogenous shock to DCI, they generally modify Item 1A's risk disclosures in 10-Ks, thus making it important to have good control (i.e., general disclosure quality) for meeting the exclusion criteria. Although we have no reason to question the quality of this control variable widely used in the accounting literature (or that of its alternative; see Online Appendix H), we cannot definitively rule out the possibility that the CL affects the cost of capital through some unobservable channel beyond the general disclosure quality of 10-Ks. For this reason, we use an alternative instrumental variable to ensure the robustness of our findings. Specifically, we focus on the occurrence of cybersecurity incidents at another firm in the same industry. The intuition for this instrument is that firms may try to clarify the measures they are taking to combat a cybersecurity threat that is known and on the radar for analysts and investors. Because this threat is posed to other firms in the same industry (we focus on firms in the same two-digit SIC code), it is unlikely that it will cause changes in the disclosure of other risk factors or ways to counter them. We collect the initial set of data breach incidents from Privacy Rights Clearinghouse (PRC) and augment it with incidents identified through a search for [cyber* (or cyber or security or cybersecurity) + (Breach or hack* or incident or catastroph*)] in LexisNexis's industry press archives. From the set of incidents identified, we retain only the incidents reported in LexisNexis's industry press archives because minor incidents without penetration to the press sphere are unlikely to elicit a response from analysts, investors, and the disclosing firms. We identified 1,082 incidents that occurred to public firms (listed in Compustat). This sample of cybersecurity incidents is sufficient to create an instrument (*peer incident*), with the value set to one for a firm in year t if at least one of its peers experienced a cybersecurity incident in the year preceding the 10-K report filing. The results are similar to that of the main analyses and are presented in column 1 of Table 4.

In addition to using peer incidents, we devise two Hausman-type instrumental variables following the existing literature (Aral et al. 2018). Specifically, we

Table 3. Further Tests of the Mechanism: DCI Interacted with Cybersecurity Investments and Institutional Holdings

Variable	*COC* (1)	*COE* (2)	*COD* (3)	*COC* (4)	*COE* (5)	*COD* (6)
DCI	−0.109***	−0.078*	−0.115***	−0.108***	−0.067**	−0.138***
	(0.024)	(0.04)	(0.022)	(0.018)	(0.030)	(0.047)
CI	−0.008	−0.009	−0.008			
	(0.006)	(0.006)	(0.006)			
CI × *DCI*	−0.055**	−0.041*	−0.062**			
	(0.025)	(0.022)	(0.029)			
IH				−0.008	−0.009	−0.008
				(0.005)	(0.006)	(0.006)
IH × *DCI*				−0.088**	−0.132***	−0.085**
				(0.04)	(0.024)	(0.038)
Informativeness	−0.086**	−0.138***	−0.081**	−0.008	−0.004	−0.006
	(0.038)	(0.021)	(0.033)	(0.005)	(0.004)	(0.005)
Informativeness × *DCI*	−0.049*	−0.049*	−0.049*	−0.048*	−0.050*	−0.050*
	(0.028)	(0.026)	(0.028)	(0.027)	(0.026)	(0.03)
Coverage	−0.008	−0.004	−0.006	−0.015	−0.018	−0.016
	(0.005)	(0.003)	(0.004)	(0.01)	(0.016)	(0.010)
Coverage × *DCI*	−0.071**	−0.049*	−0.05*	−0.073**	−0.052*	−0.052*
	(0.029)	(0.028)	(0.026)	(0.031)	(0.030)	(0.027)
Firm Size	0.002	0.002	0.002	0.002	0.002	0.002
	(0.001)	(0.002)	(0.001)	(0.001)	(0.001)	(0.001)
Assets	0.006	0.005	0.005	0.006	0.005	0.005
	(0.004)	(0.003)	(0.003)	(0.004)	(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)
R&D	−0.127***	−0.127***	−0.155***	−0.135***	−0.124***	−0.154***
	(0.026)	(0.028)	(0.035)	(0.029)	(0.024)	(0.033)
Advertising Expenditure	0.003	0.003	0.003	0.003	0.003	0.003
	(0.002)	(0.002)	(0.002)	(0.002)	(0.002)	(0.002)
IT Expenditure	−0.038	−0.035	−0.031	−0.035	−0.036	−0.032
	(0.032)	(0.022)	(0.027)	(0.021)	(0.025)	(0.02)
Forecast Error	0.004	0.005	0.005	0.004	0.005	0.005
	(0.004)	(0.003)	(0.004)	(0.002)	(0.004)	(0.004)
Analysts' Exposure	0.011	0.008	0.009	0.011	0.008	0.009
	(0.007)	(0.005)	(0.008)	(0.009)	(0.007)	(0.007)
CSR	−0.177***	−0.268***	−0.272***	−0.171***	−0.267***	−0.266***
	(0.045)	(0.068)	(0.043)	(0.035)	(0.099)	(0.046)
Noncyber Disclosure	−0.012	−0.008	−0.008	−0.012	−0.008	−0.008
	(0.007)	(0.007)	(0.007)	(0.010)	(0.007)	(0.005)
General Disclosure Quality	0.094***	0.081**	0.077***	0.004	0.008	0.007
	(0.018)	(0.035)	(0.012)	(0.003)	(0.006)	(0.006)
Wald's chi	11,533	82,999	75,748	10,745	82,143	78,091
Firm fixed effects	Yes	Yes	Yes	Yes	Yes	Yes
Year-industry fixed effects	Yes	Yes	Yes	Yes	Yes	Yes
No. of firms	1,412	1,412	1,412	1,874	1,874	1,874
Observations	11,184	11,184	11,184	16,621	16,621	16,621

Notes. This table presents cross-sectional analyses of *cybersecurity investments* (*CI*) and *institutional holdings* (*IH*). *CI* quantifies the extent of a firm's cybersecurity investment by a count of the firm's different cybersecurity-related software and technologies out of the fourteen types of cybersecurity-related software and technologies identified in the Computer Intelligence Technology Database. *IH* equals one if institutional holdings are above the sample median, and zero otherwise. The dependent variables are *cost of capital* (*COC*), *cost of equity* (*COE*), and *cost of debt* (*COD*). *COC* is a weighted average of COE and COD. The independent variable is *disclosure of cybersecurity investments* (*DCI*), which equals one if firms disclose at least one cybersecurity investment in their SEC filings in the current year, and zero otherwise. DCI is instrumented using *comment letter review*. *Coverage* is the number of financial analysts covering the firm. *Informativeness* equals one minus the cosine similarity of DCI between the focal firm and its peer firms in the same four-digit SIC code. See Online Appendix B for detailed variable definitions. All continuous variables are standardized. Standard errors are in parentheses.

***, **, and *Statistical significance at the 1%, 5%, and 10% level, respectively.

consider the industry average of DCI (*Ind_DCI*) in 10-Ks because the institutional theory of the firm suggests that firms engage in activities similar to their peers to gain legitimacy (DiMaggio and Powell 1983). Given the importance of cybersecurity threats, firms are incentivized to keep up with the cybersecurity

Table 4. Alternative Instrumental Variables

Variable	Peer incident (1)	Ind_DCI (2)	Metro_Talent (3)	Three instruments (4)	Coverage instrumented (5)
DCI	−0.084***	−0.118***	−0.113***	−0.098***	−0.130***
	(0.021)	(0.020)	(0.026)	(0.020)	(0.025)
Informativeness	−0.006 (0.005)	−0.004	−0.005	−0.006	−0.005
		(0.003)	(0.003)	(0.005)	(0.004)
Informativeness × DCI	−0.065*	−0.038	−0.059*	−0.055	−0.053*
	(0.036)	(0.023)	(0.035)	(0.036)	(0.028)
Coverage	−0.012	−0.014	−0.016	−0.012	−0.014
	(0.009)	(0.011)	(0.012)	(0.008)	(0.011)
Coverage × DCI	−0.073*	−0.069**	−0.056*	−0.097***	−0.089**
	(0.039)	(0.029)	(0.03)	(0.036)	(0.040)
Wald's chi	16,800	12,085	12,851	15,561	13,267
Controls	Yes	Yes	Yes	Yes	Yes
Firm fixed effects	Yes	Yes	Yes	Yes	Yes
Year-industry fixed effects	Yes	Yes	Yes	Yes	Yes
Year-Geo fixed effects	No	No	Yes	Yes	No
No. of firms	1,874	2,015	2,015	1,874	1,874
Observations	16,621	24,408	24,408	16,621	16,621

Notes. This table presents analyses with alternative instrumental variables. The dependent variable is *cost of capital* (*COC*). The independent variable is *disclosure of cybersecurity investments* (*DCI*), which equals one if firms disclose at least one cybersecurity investment in their SEC filings in the current year, and zero otherwise. Coefficients of control variables are not reported for brevity. In columns 1–3, DCI is instrumented using peer cybersecurity incidents, the industry average of DCI, and cybersecurity talent in metro areas where the firm's headquarters are located, respectively. In columns 2 and 3, the sample period is extended from 2006–2018 to 2000–2018, due to the expanded data availability of DCI obtained from the alternative instrumental variables. In column 4, all three instruments for DCI from columns 1–3 are included simultaneously. Sargan's chi for model 4 is 3.35 ($p = 0.34$), suggesting that the instruments are uncorrelated with error terms. In analyses instrumented using Metro_Talent, models 3 and 4, we control for Geo-year fixed effects to account for macro conditions that may affect different geographic areas differently. In column 5, coverage is instrumented using broker closures and broker mergers, following Derrien and Kecskés (2013). See Online Appendix B for detailed variable definitions. All continuous variables are standardized. Standard errors are in parentheses.

***, **, and *Statistical significance at the 1%, 5%, and 10% level, respectively.

investment disclosure norms in their industry. We use two-digit SIC codes to classify industries. In operationalizing DCI for this instrument, because we are no longer bound to CL reviews, the sample period can be extended from 2006–2018 to 2000–2018.

Additionally, we use a proprietary data set of 70 million online resumes in the United States supplemented by a major online job search platform to measure the average number of professional cybersecurity workers (*Metro_Talent*) recruited by other firms in the same metro area as the focal firm's headquarters. This number can influence DCI as it proxies the supply of local cybersecurity talent available to a firm if it intends to invest in cybersecurity. Given that cybersecurity investments require human capital support to succeed, the availability of local cybersecurity talent may increase a firm's inclination to invest in and disclose such investments. The cybersecurity talent of 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 was in cybersecurity-related projects/positions prior to recruitment. Cybersecurity talent at the metro level is then aggregated using the firm-level measure. Online Appendix F provides further details about this measure and the relevance of the two instruments. Analyses using the two Hausman-type instruments individually (columns 2 and 3 of Table 4) exhibit converging results with the main analyses. We further conduct a multi-instrument 2SLS analysis combining *peer incident*, *Ind_DCI*, and *Metro_Talent*, finding consistent effects (column 4, Table 4).

5.2. Instrumenting Analyst Coverage

Although our main identification strategy instruments DCI and controls for firm fixed effects, it is possible that a firm's extent of coverage is endogenous. For instance, when a firm faces a drastic reduction in the cost of capital, investors may be motivated to seek more scrutiny by inviting more analysts to cover the activities of the firm. Such endogeneity of coverage in our model may bias our estimates. To alleviate such concerns, we use broker closures and broker mergers as instruments that can exogenously influence the level of analyst coverage. Following Derrien and Kecskés (2013), we identify broker closures and broker mergers by examining press releases related to the brokers in the LexisNexis/Factiva database, as well as Yearbooks released by the Securities Industry Association. Each broker's portfolio of firm coverage is then

identified through records in IBES. We use these two external shocks, broker closures, and broker mergers, to build an instrument that *reduces* the extent of analyst coverage a firm might receive. A closure/merger is set to one in the event year and to zero in the year before or after the closure/merger. We add this instrument to the other instrument in our 2SLS estimation, that is, *CL_Review*. Column 5 of Table 4 reports the estimation with this added instrument. Although DCI's coefficient stays significant and negative (-0.130, $p < 0.01$), the coefficient of Coverage×DCI slightly increases in magnitude (-0.089 compared with -0.085).

5.3. Placebo and Alternative Tests

To further allay concerns over spurious trends driving the main effect of DCI on COC, we conduct a placebo test using false disclosures one year before the actual DCI. Specifically, we define a dummy variable DCI_Placebo, which equals one if the firm has a disclosure of cybersecurity investments in the following year and zero otherwise. We find that DCI_Placebo has no effect on cost of capital, cost of debt, and cost of equity (Table 5, columns $1-3$). The moderation effects of disclosure informativeness and analyst coverage also disappear. The noneffect of false disclosures further suggests that confounding events are unlikely to have driven the main findings.

Our theory is built on a core premise that DCI regulates COC due to firms' effectiveness in containing cybersecurity risks, and this occurs when the disclosure is communicated clearly and through sufficient information intermediaries. An alternative explanation is that disclosing cybersecurity risks, even merely to clarify them, can also reduce information asymmetries for investors and consequently lead to lower costs of capital. To explore whether this alternative explanation fits our findings, we replace DCI with disclosure of cybersecurity risks (DCR). Cybersecurity risk disclosures are sections of SEC reports where a firm discloses the cybersecurity risks it faces without disclosing the tangible measures taken to attenuate the risks. DCR is a dummy variable measuring whether a firm discloses cybersecurity risks but not cybersecurity investments. If this alternative explanation were valid, we would expect similar results in a model substituting DCI with DCR. Column 4 of Table 5 reports the estimates of such a model. Notably, the coefficients of DCR, DCR × Coverage, and DCR×Informativeness are all statistically insignificant. This test provides evidence that disclosing cybersecurity risks alone without

Table 5. Placebo and Alternative Tests

Variable	*COC* (1)	*COE* (2)	*COD* (3)	*COC* (4)	*COE* (5)	*COD* (6)
DCI_Placebo	−0.007	−0.003	−0.095			
	(0.064)	(0.02)	(0.102)			
DCR				0.015	0.008	0.012
				(0.013)	(0.011)	(0.032)
Informativeness	−0.006	−0.006	0.006	0.006	−0.014	−0.013
	(0.005)	(0.005)	(0.005)	(0.004)	(0.014)	(0.015)
Informativeness × DCI_Placebo	0.005	−0.004	0.007			
	(0.045)	(0.032)	(0.035)			
Informativeness × DCR				−0.013	−0.002	−0.009
				(0.010)	(0.013)	(0.011)
Coverage	−0.011	−0.011	−0.012	0.008	−0.012	−0.016
	(0.007)	(0.009)	(0.009)	(0.006)	(0.052)	(0.023)
Coverage × DCI_Placebo	0.015	−0.0021	0.012			
	(0.048)	(0.039)	(0.038)			
Coverage × DCR				−0.006	−0.000	−0.008
				(0.004)	(0.008)	(0.012)
Wald's chi	10,778	9,606	6,759	9,807	10,153	9,403
Controls	Yes	Yes	Yes	Yes	Yes	Yes
Firm fixed effects	Yes	Yes	Yes	Yes	Yes	Yes
Year-industry fixed effects	Yes	Yes	Yes	Yes	Yes	Yes
No. of firms	1,874	1,874	1,874	1,874	1,874	1,874
Observations	16,621	16,621	16,621	16,621	16,621	16,621

Notes. This table presents the results of the placebo tests. The dependent variables are *cost of capital* (*COC*), *cost of equity* (*COE*), and *cost of debt* (*COD*), respectively. The independent variable is DCI_Placebo, which equals one if firms disclose at least one cybersecurity investment in their SEC filings in the following year, and zero otherwise. The independent variable is *disclosure of cybersecurity investments* (*DCI*), which equals one if firms disclose at least one cybersecurity investment in their SEC filings in the current year, and zero otherwise. Coefficients of control variables are not reported for brevity. All analyses are instrumented using *comment letter review*. See Online Appendix B for detailed variable definitions. All continuous variables are standardized. Standard errors are in parentheses.

corresponding disclosures of tangible cybersecurity investments to counter these risks does not reduce the cost of capital. Columns 5 and 6 of Table 5 report similar estimates with COE and COD as outcome variables. This echoes with Wang et al. (2013) that security risk disclosure with risk mitigation themes are received more positively in the stock market than those without such themes.

In addition to the above analyses, we present additional robustness checks using extended samples (e.g., including financial firms) and various alternative measures for the key variables (Online Appendix G), as well as alternative control variables (Online Appendix H). The results converge qualitatively with those of the main analyses.

6. Alternative Specification: DID Estimation

6.1. Estimating the Impact of First-Time DCI

In an ideal experiment, one would randomly assign firms to disclosure and nondisclosure groups and measure any changes in the cost of capital between treated and control firms, which is not pragmatic in this context. In a quasi-random setup, we can employ a symmetric design to estimate the DID in the cost of capital between disclosing and nondisclosing firms. Ideally, both treatment and control firms should have no history of disclosure before the treatment intervention (i.e., the disclosure assignment). In practice, DCI is a strategic choice that may shift year to year. In our study, we observe instances where a disclosing firm in one year makes no disclosures in the next year(s), disclosing firms that continue disclosing until the sample period ends, and firms that switch between disclosing and not disclosing.

The closest we can achieve in terms of emulating the ideal experiment is to focus on the very first disclosure of a firm and consider it as a treatment in a quasi-experimental setup. We must, of course, identify appropriate controls to estimate the counterfactuals. Firms with prior disclosure histories but no disclosure in the specific year of interest, t, are not suitable counterfactuals. Likewise, firms that have disclosed in previous years and again in the current year are less appropriate treatment units than those disclosing for the first time. Thus, a cleaner design retains only observations of firms making their first disclosure ($Treat_i = 1$) and identifies comparable control firms with no prior disclosure history ($Treat_i = 0$). Under this design, we can rewrite Equation (1) as follows:

$$\text{Outcome}_{it} = \beta \cdot \text{Treat}_i \times \text{Post}_{it} + \gamma \cdot \text{Post}_{it} + \text{Control}_{it} + \text{FIRM}_i + \text{INDUSTRY\_YEAR} + \epsilon_{it}, \quad (2)$$

where the equation is a classic quasi-experimental design with a symmetric DID specification. In this equation, Post_{it} is equal to one if the firm is treated in year t, or if the firm is untreated in year t but is a match with a treated firm in year t. That is, a counterfactual firm is picked symmetrically in the same before and after years as the treatment group. $\text{Treat}_i \times \text{Post}_{it}$ provides the DID estimation. For instance, if a firm discloses cybersecurity investments for the first time in 2011, we measure its cost of capital in the month after the 2011 disclosure (while the cost of capital after the 2010 disclosure is retained as the measure of outcome in the pretreatment period), it is the treated unit. We then find a matching firm that has zero DCI until 2011 and measures the cost of capital for the one-month periods after its annual report releases in 2010 and 2011. This ensures that we do a symmetric matching around the treatment date (Chabé-Ferret 2015).

A classic DID estimation, such as the one above, yields unbiased estimates for the average treatment effect when two conditions are satisfied: (1) the treated and counterfactual observations follow similar pretreatment trends for the outcome variable (parallel trends assumption) and (2) the assignment to the treatment group is reasonably random (i.e., the DID term is reasonably exogenous). However, in corporate policy contexts, such as disclosure transparency, organizational choices are hardly exogenous, and prior trends in key outcomes, such as the cost of capital, likely influence firms' self-selection into treatment. The existing literature on DID designs offers a plausible solution. Particularly, Imai et al. (2023) suggest a symmetric-date matching procedure using exact matching based on historical values of the outcome variable (historical values in $t-3$, $t-2$, and $t-1$; coarsened exact matching with replacement) and then weighting the not-treated firms based on the inverse of a propensity score. The propensity score is estimated based on the historical values of time-varying covariates (e.g., the controls) in the following periods: $t-3$, $t-2$, and $t-1$.

Given the natural variation in a sample of firms, finding a match based on pretreatment values is not guaranteed. Of 814 firms that were treated at some point in our sample, we were able to find a proper match only for 574 of them. Accordingly, our DID sample includes pre- and posttreatment observations for those treated firms along with the same-year observations for their matched counterfactuals, resulting in 1,976 firm-year observations in 988 firms.[29]

Column 1 of Table 6 presents estimates from Equation (2). The DID estimate is -0.102 ($p < 0.01$), supporting Hypothesis 1.[30] The results also converge when COE and COD replace COC as the outcome variable (columns 2 and 3). Beyond strengthening causal identification, these DID results for first-time disclosure provide additional evidence on the mechanism underlying the main effect. Specifically, first-time disclosure are more likely to significantly reduce information asymmetry than subsequent ones. The fact that

Table 6. Alternative Specification: Difference-in-Differences Estimation

	First-time DCI			Heterogeneity in treatment effect			First-time DCR			DCI when the firm is raising capital	
Variable	*COC* (1)	*COE* (2)	*COD* (3)	*COC* (4)	*COE* (5)	*COD* (6)	*COC* (7)	*COE* (8)	*COD* (9)	*COE* (10)	*COD* (11)
Treat × *Post*	−0.102***	−0.078***	−0.114***	−0.052***	−0.045***	−0.063***				−0.108***	−0.121***
	(0.005)	(0.009)	(0.005)	(0.003)	(0.008)	(0.007)				(0.009)	(0.005)
Treat × *Post* × *informativeness*				−0.033***	−0.021***	−0.015***					
				(0.002)	(0.002)	(0.002)					
Treat × *Post* × *coverage*				−0.028***	−0.015***	−0.022***					
				(0.004)	(0.003)	(0.003)					
FDCR × *Post*							−0.014	−0.014	−0.015		
							(0.056)	(0.013)	(0.019)		
Post	−0.013	−0.012	0.015	0.014	−0.019	0.019	−0.002	0.005	0.013	0.023	0.017
	(0.028)	(0.029)	(0.076)	(0.023)	(0.033)	(0.088)	(0.027)	(0.031)	(0.022)	(0.034)	(0.058)
Raised Debt/Equity										0.218***	0.356***
										(0.021)	(0.042)
Wald's chi	5,968	5,007	4,781	6,238	5,187	4,965	4,233	4,402	4,253	5,165	5,412
Controls	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Firm fixed effects	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Year-industry fixed effects	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
No. of firms	988	976	960	988	976	960	1,284	1,204	1,128	292	574
Observations	1,976	1,948	1,920	1,976	1,948	1,920	2,568	2,408	2,256	624	1,348

Notes. The dependent variables are *cost of capital* (*COC*), *cost of equity* (*COE*), and *cost of debt* (*COD*). *Treat* equals one if a firm disclosed cybersecurity investments at some point in the sample period, and zero otherwise. *Post* equals one after the first disclosure of cybersecurity investments by focal and matched firms, and zero otherwise. Coefficients of control variables are not reported for brevity. Columns 1–3 of this table present difference-in-differences analyses of first-time disclosure of cybersecurity investments. Columns 4–6 present heterogeneity in the treatment effect. Columns 7–9 present alternative analyses using first-time disclosure of cybersecurity risks (FDCR) as an alternative treatment. Columns 10 and 11 present analyses of disclosures of cybersecurity investments when the firm is raising equity and debt, respectively. The additional control (Raised Debt/Equity) is the natural logarithm of raised debt or equity after the treatment period (see Figure I.2 in Online Appendix I for the design). See Online Appendix B for detailed variable definitions. All continuous variables are standardized. Standard errors are in parentheses.
*** stands for statistical significance at 1%.

first-time DCI significantly reduces COC provides additional support that the decrease in COC is due to the decrease in information asymmetry. We can estimate the heterogeneity of the treatment effect by interacting the moderating factor with $\text{Treat}_i \times \text{Post}_{it}$. Columns 4–6 show that the coefficients of $\text{Treat}_i \times \text{Post}_{it} \times \text{Coverage}_{it}$ and $\text{Treat}_i \times \text{Post}_{it} \times \text{Informativeness}_{it}$ are both negative and statistically significant, which further supports Hypothesis 2 and Hypothesis 3.

As a falsification exercise, we also estimate Equation (2) with an alternative treatment that indicates firms disclosing cybersecurity risks in their SEC filings for the first time (FDCR) without disclosing tangible cybersecurity investments to counter the risks. Columns 7–9 of Table 6 report these results. The coefficient of FDCR is −0.014 but is not statistically significant ($p > 0.10$), indicating that a general disclosure about cybersecurity does not effectively lower the cost of capital for firms. The results hold when COE and COD replace COC as the outcome.

6.2. Impact of DCI in Periods of Raising Debt/Equity

Although the COC reflects how capital markets react to the risks of investing in a firm and does so regardless of whether the firm actually raises capital in the periods for which we estimate COC (i.e., the 30-day window starting from the date of the filing of the 10-K), it is plausible that firm risk is further scrutinized when the firm actually raises capital. Specifically, when firms raise equity or debt, stakeholders will likely examine the disclosure more closely or contextualize it with complementary information, thereby further reducing information asymmetry regarding the firm's cyber risks. Therefore, the effect of DCI on COC will be more pronounced when firms raise capital.

To verify this, we need a design that allows us to do the following: first, we observe the firm's cost of capital in period $t-1$, wherein in a treatment period, the firm discloses cybersecurity investments, and subsequently, in period t the firm raises capital/debt. Then, we compare the difference in COC between treated firms and a set of reasonable counterfactuals in the two periods. We estimate Equation (2) in the sample with the aforementioned characteristics. Given that most firms in our sample disclose their cybersecurity investments in their annual reports, a design such that the treatment period is Q1 of year t, when the annual reports for year $t-1$ are disclosed, would better

capture the effect. We consider Q4 of the previous year as the before period, whereas Q2 of the current year is the after period.

To accommodate this design, we consider two samples, one with firm-year observations when the firm raises equity in Q2 (SSTK from COMPUSTAT) and one with observations when the firm raises debt in Q2 (DLTIS-DLTR from COMPUSTAT). In the first sample, the outcome variable is COE, and in the second sample, it is COD. Control covariates are measured at the quarterly level. *Treat* equals one if firms disclose a cybersecurity investment in their annual reports released in Q1 and equals zero otherwise. Counterfactuals are found in the same way as described in the previous section, except that a control observation is matched based on identical treatment history for three years (i.e., DCI in years $t-1$, $t-2$, and $t-3$). Thus, from the set of potential control observations with the same history of DCIs in the previous three years, following Imai et al. (2023), weighting is assigned to observations based on the inverse value of propensity scores based on historical values control variables (i.e., historical values from Q1, Q2, Q3, and Q4 of the previous year). *Post* equals one for observations in the current year Q2 and equals zero for observations in the previous-year Q4. Figure I.1 in Online Appendix I depicts this design.

Columns 10 and 11 of Table 6 present the results of these estimations. The DID estimates (*Treat* × *Post*) show effect sizes that are significantly larger than those in the estimates of DCI in our observational models. This is consistent with the underlying mechanism laid out earlier. Firms' financing needs prompt additional scrutiny from capital markets, leading investors to parse the signals sent through DCI, which in turn reduces information asymmetry between investors and firms and, consequently, lowers the costs of equity and debt.

To conclude, both the CL review (IV) and DID approaches have respective strengths and weaknesses. The CL review approach shocks DCI but reduces the general disclosure quality (which we address by controlling the variable), whereas the DID approach provides a clean setting, but the first-time DCI requirement and the matching criteria naturally reduce the sample size. Nevertheless, across a battery of different specifications, results converge in both direction and magnitude.

7. Conclusions

In evaluating the effect of disclosing cybersecurity investments, this paper moves beyond short-term equity-market reactions (Gordon et al. 2010, Bose and Leung 2019) and examines how such disclosures improve firms' access to capital. This represents a fundamental shift in how cybersecurity disclosures are understood and interpreted, moving the focus from sentiment-based and often transitory effects to more stable and substantial influences on firms' access to vital resources such as capital. Although market return measures such as CAR capture both cash flow and discount (risk) factor news, the cost of capital is a direct measure of risk. Its tie with DCIs thus reveals how capital markets view cybersecurity as a fundamental component of public firms' risk structure. Because the payoff structures of debt and equity markets differ (downside protection versus upside participation), the cost of capital offers a more comprehensive view of firm risks by integrating information from both the markets. CAR can also be influenced by prior market anticipation of disclosures and potential market overreaction or underreaction (Chan 2003), whereas cost of capital is less affected by the timing and measurement window. In short, executives rely more on the cost of capital, which serves as a key input in valuation models like discounted cash flow analysis. A higher cost of capital reduces the present value of future cash flows, which decreases firm value. Managers focus on controlling factors that affect firm value over time, and the cost of capital, unlike price fluctuations due to passing perceptions, is a core element in that equation.

Building on prior literature (Gordon et al. 2010, Bose and Leung 2019), this study further delineates how signals sent through periodic reports undergo a process of information intermediation that ultimately improve firms' access to capital. In doing so, we provide unique evidence that supports the presence of this information intermediation process in the case of cybersecurity investment disclosures. First, we show that firms with more financial analyst coverage and a higher level of institutional holdings are more likely to benefit from disclosing cybersecurity investments. Analysts are information intermediaries, and institutional investors often possess the resources to conduct further information discovery triggered by disclosure signals. In addition to providing fresh evidence that cybersecurity investment disclosures are picked up by information intermediaries, this finding reveals the type of firms that can reap more value from disclosing cybersecurity investments. Importantly, we show that informative disclosures, that is, those significantly different from peer disclosures and historical disclosures, are tied to better access to capital, suggesting that boilerplate disclosures have limited effect. This is rare evidence regarding the limitations of boilerplate disclosures, which are common in the cybersecurity domain. Further consistent with the information intermediation mechanism, we show the level of actual cybersecurity investments plays a key role in converting disclosure signals into tangible capital access benefits. This suggests that disclosures are subject to additional information discovery as part of the intermediation process,

and that without a demonstrable commitment to cybersecurity investments, such disclosures may not yield the expected benefits. This echoes prior studies on stock market reactions to cyber risk disclosures with risk-mitigation themes (Wang et al. 2013) and on the effectiveness of substantive cybersecurity investments in preventing data breaches (Angst et al. 2017).

Our study is not without limitations. Because our sample consists of U.S. firms, and cybersecurity disclosure mandates vary across different countries, the effect on cost of capital should be generalized with caution. In revealing the underlying mechanism, we have adopted analyst coverage as one of the moderators. Although the number of analysts covering a firm is observable, we do not have access to databases containing analyst reports. As a result, we are unable to perform content analysis on these reports, which limits our understanding of the information intermediation process. Moreover, although the study measures firms' in-house IT infrastructure, many organizations are shifting toward cloud computing, which may attenuate the effect of cybersecurity investment disclosures on capital market assessments of firm risk. With the looming disruptions of artificial intelligence and quantum computing on cybersecurity, future studies will also need to account for the impact of latest technologies on cybersecurity risk. With increasing regulatory attention on cybersecurity, recent years have seen the introduction of stricter disclosure requirements. For instance, the SEC's 2023 rule mandates "registrants to disclose material cybersecurity incidents they experience and to disclose on an annual basis material information regarding their cybersecurity risk management, strategy, and governance."[31] Building on voluntary cybersecurity disclosure, future research can leverage these regulatory changes to examine the effect of more stringent cybersecurity disclosure requirements on capital markets and beyond.

Acknowledgments

The authors thank the senior editor, associate editor, and reviewers for clear guidance and constructive feedback and Sezgin Ayabakan, John D'Arcy, seminar participants at the CMU-Pitt Seminar on Information Technology & Economics, University of Delaware, City University of Hong Kong, and participants of the 2020 Workshop on the Economics of Information Security for insightful comments and suggestions.

Endnotes

[1] See https://www.gartner.com/en/newsroom/press-releases/2024-08-28-gartner-forecasts-global-information-security-spending-to-grow-15-percent-in-2025.

[2] SEC guidance on cybersecurity disclosures in 2011 and 2018: https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm, https://www.sec.gov/files/rules/interp/2018/33-10459.pdf.

[3] Online Appendix A provides an illustration of the low rate of disclosures of cybersecurity investments.

[4] 2023 SEC rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies: https://www.sec.gov/corpfin/secg-cybersecurity.

[5] For example, Equifax faced class action lawsuits over its 2017 data breach, with plaintiffs citing the company's own claims of having "strong data security": https://natlawreview.com/article/court-finds-cybersecurity-related-claims-sufficient-securities-class-action.

[6] Awareness costs are expenses incurred by investors to monitor for and become aware of the existence of new disclosures. Acquisition costs are expenses related to obtaining and accessing the content of disclosures. Integration costs are expenses associated with analyzing, interpreting, and incorporating the information from disclosures into investment decisions.

[7] The percentage of financial firms and real estate firms excluded relative to the total number of firms is approximately 2%.

[8] In matching firms with CITDB, a semiautomatic approach was followed, where first a simple word match (after excluding "Inc.," "Corp.," etc. from firm names) was conducted and exact matches were identified. Then, the rest of the firms were manually matched to the CITDB data set.

[9] This roughly translates to 8.6 observations for each firm, and therefore the panel is not balanced. This is mainly due to a firm being delisted (e.g., because of mergers, acquisitions, or bankruptcies) or CITDB not profiling a firm in certain years.

[10] The measures, citations, and data sources for each variable are summarized in Online Appendix B.

[11] Online Appendix D presents evidence of the extent of variations of the cost of debt (COD) in the sample.

[12] We acknowledge that CITDB has certain limitations. McElheran (2014) suggests that a firm's headquarters may not be aware of IT adoptions at the establishment level. We do not possess the proprietary data on the IT purchasing authority to address this limitation.

[13] As Chen et al. (2015) explain, value-weighting nonmissing item ratios in income statements are problematic because the operating expense group alone accounts for about 90% of the weight when using sales as the denominator of the weight ratio.

[14] Total assets are deflated by the GDP deflator for nonresidential fixed investments and depreciated by 5%.

[15] The GDP deflator for nonresidential fixed investments is used to deflate R&D and ADV; missing values are replaced by zero, following prior studies. The base year for all deflations is the year 2000.

[16] Although we have access to CITDB from 2000 to 2018, our access to InformationWeek 500 rankings is limited only to the 2000–2010 period. Still, it is notable that we find that 81% of the public firms appearing in the InformationWeek 500 rankings are present in CITDB.

[17] See https://www.sec.gov/news/speech/2008/spch111708wc-slides.pdf.

[18] Figure E.1 in Online Appendix E depicts the distributions of DCI for firms with CL reviews.

[19] Figure E.2 in Online Appendix E provides a timeline depiction of the CL review process. Other figures in Online Appendix E provide additional support regarding the validity of the instrument, particularly the exclusion criteria.

[20] See https://www.sec.gov/news/press/2004-89.htm.

[21] See https://www.sec.gov/divisions/corpfin/cfannouncements/edgarcorrespondence.htm.

[22] In our sample, as shown in Figure E.3 of the Online Appendix E, 21% of those receiving CLs move from no DCI pre-CL to some level of DCI.

[23] We present a plethora of additional analyses in the Online Appendices to further evaluate the robustness of our findings.

[24] Main analyses without instrumentation shows a similar relationship with much larger effect size (Table E.5 in Online Appendix E).

[25] The standard deviations of COC and its mean in model 1's sample are 0.065 and 0.085, respectively, and therefore firms with DCI = 1 have, on average, $0.099\left(\frac{0.065}{0.085}\right) \approx 7.6\%$ lower COC.

[26] In the Wu-Hausman's diagnostic test for the model in column 7 of Table 2, panel B, the *F*-value is 47.2 ($p < 0.001$).

[27] On average, a 1% increase in coverage will increase the effect of DCI on the cost of capital by 0.333%. Similarly, on average, a 1% increase in informativeness leads to a 0.011% increase in the main effect. Given that informativeness is only observable when DCI = 1, we conducted an additional analysis where we treat DCI as the choice variable in a Heckman selection model (Table H.5, Online Appendix H). Notably, the inverse Mills ratio is insignificant in the second stage, suggesting no support for the presence of selection bias. The results reaffirms that informativeness negatively affects COC.

[28] The categorization of these software and technology items as cybersecurity related is directly obtained from the extended installation tables provided by the Aberdeen Group.

[29] Table I.4 in Online Appendix I presents the results of models with a set of different matching approaches.

[30] Table I.1 in Online Appendix I presents a relative time estimation confirming the parallel trends assumption, with all pretreatment effects being insignificant and posttreatment effects showing significance consistent with Equation (2) estimations. Figure I.1 illustrates the relative time DID estimate. Table I.2 presents alternative DID estimations.

[31] See https://www.sec.gov/news/press-release/2023-139.

References

Agarwal S, Ghosh P, Ruan T, Zhang Y (2024) Transient customer response to data breaches of their information. *Management Sci.* 70(6):4105–4114.

Akins BK, Ng J, Verdi RS (2012) Investor competition over information and the pricing of information asymmetry. *Accounting Rev.* 87(1):35–58.

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

Angst CM, Block ES, D'arcy J, Kelley K (2017) When do IT security investments matter? Accounting for the influence of institutional factors in the context of healthcare data breaches. *MIS Quart.* 41(3):893–916.

Aral S, Bakos Y, Brynjolfsson E (2018) Information technology, repeated contracts, and the number of suppliers. *Management Sci.* 64(2):592–612.

Argote L, Greve HR (2007) A behavioral theory of the firm—40 years and counting: Introduction and impact. *Organ. Sci.* 18(3): 337–349.

Barber B, Lehavy R, McNichols M, Trueman B (2001) Can investors profit from the prophets? Security analyst recommendations and stock returns. *J. Finance* 56(2):531–563.

Bardhan I, Krishnan V, Lin S (2013) Research note—Business value of information technology: Testing the interaction effect of IT and R&D on Tobin's Q. *Inform. Systems Res.* 24(4): 1147–1161.

Barth ME, Beaver WH, Landsman WR (2001) The relevance of the value relevance literature for financial accounting standard setting: Another view. *J. Accounting Econom.* 31(1–3):77–104.

Barth ME, Konchitchki Y, Landsman WR (2013) Cost of capital and earnings transparency. *J. Accounting Econom.* 55(2–3):206–224.

Bates TW, Kahle KM, Stulz RM (2009) Why do US firms hold so much more cash than they used to? *J. Finance* 64(5):1985–2021.

Bennedsen M, Nielsen KM, Pérez-González F, Wolfenzon D (2007) Inside the family firm: The role of families in succession decisions and performance. *Quart. J. Econom.* 122(2):647–691.

Benner MJ (2010) Securities analysts and incumbent response to radical technological change: Evidence from digital photography and internet telephony. *Organ. Sci.* 21(1):42–62.

Bertomeu J, Vaysman I, Xue W (2021) Voluntary versus mandatory disclosure. *Rev. Accounting Stud.* 26(1):658–692.

Bhushan R (1989) Firm characteristics and analyst following. *J. Accounting Econom.* 11(2–3):255–274.

Billett MT, Xue H (2007) The takeover deterrent effect of open market share repurchases. *J. Finance* 62(4):1827–1850.

Blankespoor E, deHaan E, Marinovic I (2020) Disclosure processing costs, investors' information choice, and equity market outcomes: A review. *J. Accounting Econom.* 70(2–3):101344.

Bose I, Leung ACM (2019) Adoption of identity theft countermeasures and its short-and long-term impact on firm value. *MIS Quart.* 43(1):313–327.

Bradshaw MT, Richardson SA, Sloan RG (2006) The relation between corporate financing activities, analysts' forecasts and stock returns. *J. Accounting Econom.* 42(1–2):53–85.

Brown SV, Tucker JW (2011) Large-sample evidence on firms' year-over-year MD&A modifications. *J. Accounting Res.* 49(2):309–346.

Chabé-Ferret S (2015) Analysis of the bias of matching and difference-in-difference under alternative earnings and selection processes. *J. Econom.* 185(1):110–123.

Chan WS (2003) Stock price reaction to news and no-news: Drift and reversal after headlines. *J. Financial Econom.* 70(2):223–260.

Chen S, Matsumoto DA (2006) Favorable versus unfavorable recommendations: The impact on analyst access to management: Provided information. *J. Accounting Res.* 44(4):657–689.

Chen T, Dong H, Lin C (2020) Institutional shareholders and corporate social responsibility. *J. Financial Econom.* 135(2):483–504.

Chen S, Miao B, Shevlin T (2015) A new measure of disclosure quality: The level of disaggregation of accounting data in annual reports. *J. Accounting Res.* 53(5):1017–1054.

Chen T, Jeffrey Hu Y, Rahman M, Sun J (2021) The effects of sister-store presence and market competition on product assortment: Evidence from book retailing. *Service Sci.* 13(3):155–171.

Cheng B, Ioannou I, Serafeim G (2014) Corporate social responsibility and access to finance. *Strategic Management J.* 35(1):1–23.

Chi F, Hwang BH, Zheng Y (2024) The use and usefulness of big data in finance: Evidence from financial analysts. *Management Sci.* 71(6):4599–4621.

Cohen L, Malloy C, Nguyen Q (2020) Lazy prices. *J. Finance* 75(3):1371–1415.

Cutler J, Davis AK, Peterson K (2019) Disclosure and the outcome of securities litigation. *Rev. Accounting Stud.* 24(1):230–263.

D'Arcy J, Adjerid I, Angst CM, Glavas A (2020) Too good to be true: Firm social performance and the risk of data breach. *Inform. Systems Res.* 31(4):1200–1223.

Derrien F, Kecskés A (2013) The real effects of financial shocks: Evidence from exogenous changes in analyst coverage. *J. Finance* 68(4):1407–1440.

Dhaliwal DS, Li OZ, Tsang A, Yang YG (2011) Voluntary nonfinancial disclosure and the cost of equity capital: The initiation of corporate social responsibility reporting. *Accounting Rev.* 86(1):59–100.

DiMaggio PJ, Powell WW (1983) The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. *Amer. Sociol. Rev.* 48(2):147–160.

Duro M, Heese J, Ormazabal G (2019) The effect of enforcement transparency: Evidence from SEC comment-letter reviews. *Rev. Accounting Stud.* 24(3):780–823.

Easley D, O'Hara M (2004) Information and the cost of capital. *J. Finance* 59(4):1553–1583.

Fama EF, French KR (1997) Industry costs of equity. *J. Financial Econom.* 43(2):153–193.

Faulkender M, Petersen M (2012) Investment and capital constraints: Repatriations under the American Jobs Creation Act. *Rev. Financial Stud.* 25(11):3351–3388.

Fazzini K (2018) Moody's is going to start building the risk of a business-ending hack into its credit ratings. *CNBC* (November 12), https://www.cnbc.com/2018/11/12/moodys-to-build-business-hacking-risk-into-credit-ratings.html.

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

Francis J, Nanda D, Olsson P (2008) Voluntary disclosure, earnings quality, and cost of capital. *J. Accounting Res.* 46(1):53–99.

Frank MZ, Shen T (2016) Investment and the weighted average cost of capital. *J. Financial Econom.* 119(2):300–315.

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

Hall BH, Lerner J (2010) The financing of R&D and innovation. Arrow KJ, Intriligator MD, eds. *Handbook of the Economics of Innovation* (Elsevier, Amsterdam), 609–639.

Havakhor T, Sabherwal R, Steelman ZR, Sabherwal S (2019) Relationships between information technology and other investments: A contingent interaction model. *Inform. Systems Res.* 30(1):291–305.

He JJ, Tian X (2013) The dark side of analyst coverage: The case of innovation. *J. Financial Econom.* 109(3):856–878.

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

Heese J, Khan M, Ramanna K (2017) Is the SEC captured? Evidence from comment-letter reviews. *J. Accounting Econom.* 64(1):98–122.

Hennessy CA, Whited TM (2007) How costly is external financing? Evidence from a structural estimation. *J. Finance* 62(4):1705–1745.

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

Huang HH, Wang C (2020) Do banks price firms' data breaches? *Accounting Rev.* 96(3):261–286.

Hubbard R (1998) Capital-market imperfections and investment. *J. Econom. Literature* 36(1):193–225.

Imai K, Kim IS, Wang EH (2023) Matching methods for causal inference with time-series cross-sectional data. *Amer. J. Political Sci.* 67(3):587–605.

Jia N, Rai A, Xu SX (2020) Reducing capital market anomaly: The role of information technology using an information uncertainty lens. *Management Sci.* 66(2):979–1001.

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

Kisgen DJ (2009) Do firms target credit ratings or leverage levels? *J. Financial Quant. Anal.* 44(6):1323–1344.

Kvochko E, Pant R (2015) Why data breaches don't hurt stock prices. *Harvard Bus. Rev.* (March 31), https://hbr.org/2015/03/why-data-breaches-dont-hurt-stock-prices.

Kwon J, Johnson ME (2014) Proactive versus reactive security investments in the healthcare sector. *MIS Quart.* 38(2):451–471.

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

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

Li WW, Leung ACM, Yue WT (2023) Where is IT in information security? The interrelationship among IT investment, security awareness, and data breaches. *MIS Quart.* 47(1):317–342.

Lintner J (1975) Inflation and security returns. *J. Finance* 30(2): 259–280.

Luo X, Wang H, Raithel S, Zheng Q (2015) Corporate social performance, analyst stock recommendations, and firm future returns. *Strategic Management J.* 36(1):123–136.

Marquis C, Toffel MW, Zhou Y (2016) Scrutiny, norms, and selective disclosure: A global study of greenwashing. *Organ. Sci.* 27(2):483–504.

Marsh P (1982) The choice between equity and debt: An empirical study. *J. Finance* 37(1):121–144.

McElheran K (2014) Delegation in multi-establishment firms: Evidence from IT purchasing. *J. Econom. Management Strategy* 23(2): 225–258.

Merkley KJ (2014) Narrative disclosure and earnings performance: Evidence from R&D disclosures. *Accounting Rev.* 89(2):725–757.

Mithas S, Whitaker J, Tafti A (2017) Information technology, revenues, and profits: Exploring the role of foreign and domestic operations. *Inform. Systems Res.* 28(2):430–444.

Nagle F (2019) Open source software and firm productivity. *Management Sci.* 65(3):1191–1215.

Roberts MR, Whited TM (2013) Endogeneity in empirical corporate finance. Arrow KJ, Intriligator MD, eds. *Handbook of the Economics of Finance* (Elsevier, Amsterdam), 493–572.

Robins J, Wiersema MF (1995) A resource-based approach to the multibusiness firm: Empirical analysis of portfolio interrelationships and corporate financial performance. *Strategic Management J.* 16(4):277–299.

Saunders A, Brynjolfsson E (2016) Valuing information technology related intangible assets. *MIS Quart.* 40(1):83–110.

Sharfman MP, Fernando CS (2008) Environmental risk management and the cost of capital. *Strategic Management J.* 29(6):569–592.

Shroff N, Sun AX, White HD, Zhang W (2013) Voluntary disclosure and information asymmetry: Evidence from the 2005 Securities Offering Reform. *J. Accounting Res.* 51(5):1299–1345.

Wang T, Kannan KN, Ulmer JR (2013) The association between the disclosure and the realization of information security risk factors. *Inform. Systems Res.* 24(2):201–218.

Verrecchia RE (2001) Essays on disclosure. *J. Accounting Econom.* 32(1–3):97–180.