Journal of Forensic and Investigative Accounting
Volume 15: Issue 2, July–December 2023

Cybersecurity Risk Disclosure Quality: Does it Affect the Cost of Debt?

Dan Harris
Cemil Kuzey
Christine Naaman
*Najib Sahyoun**

I. Introduction

This study analyzes the association between cybersecurity risk disclosure and the cost of debt. We focus on the distinctive characteristics of cybersecurity disclosure—total number of words, readability complexity level, and number of litigious words—on creditors' required rate of return. In recent years, the quantity and severity of cybersecurity threats have risen significantly (Cheong *et al.*, 2021). Perpetrators of cyberattacks include belligerent nations, independent hackers, organized crime, and malicious insiders (Grove and Clouse, 2020). Numerous corporations' data and information have not only been hacked and viewed by unauthorized entities, but also stolen and shared with adversaries (SEC, 2011a; 2018).

Prominent cybersecurity breaches include the: 1) July 2017 Equifax breach of 145 million individuals' personal information; 2) May 2017 WannaCry ransomware attack across 150 countries that locked down over 300,000 machines; and 3) July 2019 Capital One breach that affected 106 million customers' data (Larson, 2017; Capital One, 2019). In 2019, hackers seized parts of the computer systems that run the City of Baltimore's government. Through a ransomware attack, hackers remotely encrypted critical files and demanded a ransom. The City took systems offline to keep the ransomware from spreading, but only after the attack had taken down voicemail, email, a parking-fines database, and a payment system for water bills, property taxes, and vehicle citations. Additionally, at least 1,500 pending home sales were delayed. The digital ransom note demanded three Bitcoins (then, nearly $24,000) per system or 13 Bitcoins in total (about $102,000 at the time) to unlock the seized files (Chokshi, 2019). In 2019, Springhill Medical Center was attacked by hackers who demanded a ransom. This attack affected patients' records, cutting off the equipment that relay information on fetal heartbeats to the nurses' desk. Tragically, a baby in distress died without nurses having acted, since the equipment was not charting babies' heartbeats. This attack is considered to be the first alleged ransomware leading to a death (Poulsen *et al*., 2021). A 2021 ransomware attack on a software package developed by Kaseya, a U.S. information-technology firm, affected between 800 and 1,500 businesses globally, paralyzing hundreds of them across five continents (Satter, 2021).

Breaches can have significant adverse effects, including the loss of customers, suppliers, and future growth opportunities. Nearly 20% of consumers will not purchase products or services from a company that has reported a cybersecurity breach (Sheneman, 2017). Lost business (i.e., customer turnover, lost revenue from system downtime, and the higher cost of acquiring new business because of diminished reputation) accounted for 38% of the overall average data breach cost. For 2021, the average cost of a mega breach, breaches of between 50 million and 65 million records, was $401 million, an increase from $392 million in 2020 (Ponemon Institute, 2021).

In 2011, the SEC issued Corporate Finance Disclosure Guidance: Topic No. 2 (SEC, 2011a; 2011b) that states that in their SEC filings, public companies should disclose the risks of cyber incidents that "are among the most significant factors that make an investment in the company speculative or risky." Consistent with the disclosure of other operational and financial risks, disclosures of firms' risk of potential material cyberattacks should include specific information about the nature of the risks and how each risk affects the company's business. Public companies should disclose both the risks of potential cyber-attacks and the known material cyber incidents that have already occurred, including the potential costs and consequences (SEC, 2011a; SEC, 2011b). After both the 2017 Equifax breach and SEC EDGAR-database breach, the SEC issued updated guidance directing public companies to prepare disclosures of cybersecurity risks (SEC, 2018). The 2018 guidance expanded the SEC's 2011 cybersecurity guidance; two topics were addressed. First, the SEC reemphasized the importance of cybersecurity procedures and controls to enable timely and accurate disclosures of cybersecurity risks

*The authors are, respectively, Associate Professor of Accounting, Associate Professor of Computer Information Systems, and Assistant Professors of Accounting at Murray State University.

and incidents. Second, the SEC prohibited the insider trading of cybersecurity incidents (Calderon and Gao, 2021; Gao *et al.*, 2020). Based on the 2018 guidance, companies are recommended to review the following areas when evaluating the cybersecurity risks and cybersecurity incidents for disclosures: 1) the occurrence of cyber incidents; 2) the probability of potential cyber incidents; 3) the preventive actions to reduce cybersecurity risks; 4) the cybersecurity risks of companies' nature of business or operation; 5) the costs of maintaining cybersecurity risks such as insurance coverage; 6) the reputational harm; 7) the costs related to existing or potential new regulation; and 8) the litigation risks (SEC, 2018). Another noticeable difference is that the 2018 guidance emphasized that companies should avoid generic cybersecurity-related disclosure and boilerplate language and provide specific information that is useful to investors (SEC, 2018).

The SEC advises firms to avoid legalistic, overly complex presentations, since they make the substance of the disclosure difficult to understand (SEC, 1998). "Ruthlessly eliminate jargon and legalese. Instead, use short, familiar words to get your points across" (SEC, 1998 p. 36). "A plain-English document uses words economically and at a level the audience can understand. Its sentence structure is tight. Its tone is welcoming and direct. Its design is visually appealing." It is easy to read and "looks like it's meant to be read" (SEC, 1998 p. 11). Firms' use of concrete language increases investors' comfort in their ability to evaluate an investment (Rjiba *et al.*, 2021). Retail investors are more willing to hold stock in firms that have more readable financial reports. If information is conveyed in a manner that is too complex for its intended audience, it can result in misunderstanding, the impairment of reporting quality, or reduction of the decision-making abilities of the target audience (Jackson *et al.*, 2019).

Sheneman (2017) believes that the cost of debt is a strong metric to evaluate cybersecurity breach incidents. First, the debt markets rely heavily on financial-statement information, particularly the private loan market, which handles over 50% of debt financing in the U.S. Second, due to the payoff structure of debt, creditors are risk averse, which incentivizes them to examine a debtor's risks. Third, the elements of the cost of debt measure are readily available and specified in negotiated loan agreements. Accordingly, the cost of debt measure has intrinsically less noise than an extrapolated cost-of-equity measure.

We obtain data from Gao *et al.* (2020) that consists of cybersecurity risk disclosures from 2007 to 2018. We investigate the characteristics of the firms' cybersecurity risk disclosure impact on cost of debt. This study uses a generalized method of moments (GMM)-based dynamic panel regression analysis to test our models. We find that lower cybersecurity risk disclosure quality, measured in higher number of words, higher complexity in reading, and higher number of litigious words, leads to higher cost of debt. Our results suggest that when lenders are faced with lower quality cybersecurity risk disclosures, they tend to factor it as a higher risk or higher potential for future cybersecurity incidents. Therefore, the cost of debt increases.

Our study presents several contributions. First, there is limited research on cybersecurity risk disclosure. Most of the existing research has examined cybersecurity breach incidents, rather than disclosures (Calderon and Gao, 2021). In recent years, the SEC has emphasized the importance of businesses disclosing cybersecurity risks, as manifested by the issuance of requirements in 2011 and 2018 (SEC, 2011; 2018). Cybersecurity risk disclosure is informative for investors and creditors, since it can reveal the internal control weaknesses of a firm's overall control environment in general, as well as the internal controls' effectiveness related to financial-statement reliability in particular (Calderon and Gao, 2021; Li *et al.*, 2018). Thus, our study sheds light on a topic that affects not only cybersecurity risk, but also the overall control environment and financial-statement reliability. Second, this article analyzes the association between cybersecurity risk disclosure characteristics and cost of debt. To our knowledge, this is the first study analyzing the impact of cybersecurity risk disclosure quality on cost of debt. Calderon and Gao (2021) analyze the impact of cybersecurity risk disclosure on auditor fees. Their study focuses on the audit risk that is manifested through the auditors' risk assessment and fee's structure. We extend their results by investigating the impact of these disclosures on the lending market which has its own characteristics and differs from the audit market or equity market. Third, our empirical results are enriching for the accounting-disclosure literature. We show that higher disclosure quality leads to favorable outcomes in cost of debt. Thus, our study has policy implications for regulators' emphasis that cybersecurity risk disclosure should be tailored to firms' particular risks and incidents, avoid both boilerplate and litigious language, and be written in a clear and informative way (SEC, 2018). Fourth, our study examines the debt market which is studied much less than the equity market in the literature, even though the debt market has considerable size and has grown significantly in recent years (Bonsall and Miller, 2017). In 2020, the U.S. debt market grew to $50.1 trillion, representing a significant portion of the capital market (SIFMA, 2021).

The rest of the study is organized as follows. Section II presents the literature review and hypotheses development. Section III discusses the study's research design. Section IV analyzes the results. Finally, section V concludes the paper.

II. Literature Review and Hypotheses Development

General Overview of Cybersecurity

In a global world where information travels through cyberspace, effective information management is paramount. It involves recognition of expanding vulnerabilities, including cyber threats and information warfare. Due to organizations' pervasive use of information technology and the consequent rise in cybersecurity threats, cybersecurity has become a vital issue for virtually every organization, regardless of size (Cheong *et al.*, 2021). Many industries depend on the Internet, including telecommunications, banking and finance, energy, transportation, the military, and other essential government services. As both the public and private sectors have become more dependent upon Web-based technologies and networks for their financial-management systems, they have become increasingly susceptible to threats (Gansler and Lucyshyn, 2005).

From 2015 to 2016, ransomware attacks quadrupled to 4,000 per day (Department of Justice, 2017). U.S. data breaches grew from 1,093 million in 2016 to 1,579 million in 2017 (Jackson *et al.*, 2019). Eighty-nine percent of firms surveyed in 2017 reported at least one cyber incident (Kroll, 2018). In 2021, the average total cost of data breach increased from $3.86 million to $4.24 million in the U.S. which is considered the largest increase in the last seven years (Ponemon Institute, 2021). Firms are more likely to experience cyberattacks if they are: (1) larger; (2) a Fortune 500 company; (3) financially less constrained; (4) more highly valued; (5) owners of significant intangible assets; and (6) operating in less competitive industries (Kamiya *et al.*, 2018). According to the World Bank's report in 2018, the financial-services industry was attacked more than any other industry (Haapamäki and Sihvonen, 2019).

Ransomware costs in the United States increased to over $8 billion in 2018 from $25 million in 2014 (Morgan, 2018). As of 2021, the U.S. continued to have the highest global cost per cybersecurity breach, with costs rising to $8.64 million per event. Further, the average breach took 280 days to identify and contain (Jiang *et al.*, 2021). Additional potential cyberattack costs include: remediation costs, including liability for stolen assets/information, repairs to damaged systems, and incentives to customers/business partners to prevent the loss of business and/or maintain relationships, cybersecurity protection costs, including significant organizational changes, new technologies, training, and third-party consultants, litigation costs and legal liability, including that to local, national, and international regulatory authorities, increased insurance premiums, and damage to the company's stock price and long-term shareholder value (SEC, 2018).

Both the public and business community are concerned, since cyberattacks have exposed sensitive personal information, caused business disruptions, and stolen trade secrets, particularly the high-profile data breaches involving Equifax, Sony, and Target (Li *et al.*, 2018). Investors have become increasingly concerned about firms' levels of exposure to cybersecurity risks (Spanos and Angelis, 2016). Companies that suffer a data breach underperform the NASDAQ by an average of 42% in the subsequent three-year period (O'Connell, 2017). A study by Kamiya *et al.* (2018) find that only two months following the announcement of its 2017 cyberattack, Equifax's stock price was lower by almost 25% than before the attack. Also, they find a significant mean cumulative abnormal return (CAR) of −0.84% during the three-day window around a cyberattack announcement, translating into an average value loss of $495 million per attack. These CARs are particularly significant (−1.09%) for firms whose cyberattacks result in a loss of financial information (i.e., social security numbers, bank account, and/or credit card information), as opposed to those that resulted in the loss of personally identifiable non-financial information (i.e., including driver license, medical record, and/or e-mail information). Furthermore, their results suggest particularly negative CAR amongst older firms and those without evidence of board attention to risk management.

Cybersecurity Risk Disclosure

As a result of a cybersecurity breach, companies' assets and customer information can be compromised, as well as their reputations, resulting in significant remediation costs and potential legal liability. Stakeholders are increasingly concerned about cybersecurity, thus demanding additional information about cybersecurity incidents, specifically those that involve actual breaches (Swift *et al.*, 2020).

The intent of cybersecurity disclosure is to provide precise information to stakeholders about the level and scope of cybersecurity risks. While risk disclosures are mandatory, they can also be vague. Management strategically formulates the

wording of disclosures, considering the possible costs and incentives. While regulators have put increased pressure on firms that fail to make appropriate cybersecurity risk disclosures, researchers and practitioners have questioned the disclosures' informativeness. Comprehension of cybersecurity risk disclosure is critical, since it can help investors evaluate a firm's cybersecurity risk and provide regulators with information about whether additional legislative rules are necessary (Bennett, 2015; Li *et al.*, 2018).

For companies to assess cybersecurity risks, the AICPA created an attestation guide focusing upon cybersecurity description and control criteria (Grove and Clouse, 2020). Risk can be pervasive, which affects the integrity of the entire financial-information system, or specific, which impacts individual applications or data segments (Deloitte, 2020). Regardless, cybersecurity risk will likely impact a financial-reporting system's general controls and application controls, thereby increasing the likelihood of material misstatement (Smith *et al.*, 2019).

"The AICPA emphasized that its cybersecurity risk management reporting framework is a crucial first step toward enabling a consistent, market-based, business-based solution for companies to communicate successfully with key stakeholders on how they are managing cybersecurity risk" (Haapamäki and Sihvonen, 2019). While the SEC Commissioners unanimously approved the 2018 SEC guidance, several of them believed that the new guidance fell short, including SEC Commissioner Kara Stein, who stated that she is "disappointed with the Commission's limited action" (Stein, 2018). SEC Chairman Jay Clayton stated that since the cybersecurity landscape and associated risks are evolving every day, further guidance might be needed as the SEC continues to evaluate the developments (Clayton, 2018). Since the nature of cybersecurity risks could vary widely and affect business entities in different ways, the SEC not only expects companies to tailor their disclosures to their specific cybersecurity risks, but also anticipates that different risks will be reported in different sections of the 10-K, including Item 1A Risk Factors, Item 7 MD&A, Item 8 Financial Statements and Supplementary Data, and Item 9A Controls and Procedures (SEC, 2011a; 2011b; 2018).

Debt Market

The United States corporate bond market has grown significantly since 2015 (Bonsall and Miller, 2017). It is estimated to be around $50.1 trillion in 2020 (SIFMA, 2021). Based on the costly contracting hypothesis, loan contracts establish covenants to prevent borrowers from actions that reduce the value of lenders' claims. Loan covenants can restrict debtors' behavior, both in protecting creditors from losses and reducing moral-hazard costs (Sheneman, 2017). Loan covenants are alternatives to direct monitoring, since their violation can lead to the transfer of control rights from debtors to creditors upon violation (Dichev and Skinner, 2002; Dyreng *et al.*, 2017). Creditors can use debtor information both to predict and price the likelihood of a cybersecurity breach. Additionally, lenders may try to diversify potential cybersecurity breaches across their loan portfolios (Sheneman, 2017). "Incomplete contracting theory recognizes that it is not feasible for lenders and borrowers to contract upon all potential states of the world because some information is unknown and unknowable" (Knight, 1921). Such incomplete information and imperfect prospective knowledge are included in capital pricing, since it is a calculation based on anticipated potential outcomes, cash flows, and the risk assessment (Stiglitz and Weiss, 1981).

Prior studies have analyzed the debt market. For a breached firm, the cost of debt is twenty-five basis points higher on average than for non-breached firms. This result represents a 16% increase in loan spread, relative to the pre-breach average spread of 154 basis points over LIBOR (Sheneman, 2017). After receiving a modified audit opinion, a firm's loan spread increases by 17 basis points on average (Chen *et al.*, 2016). Firms that exhibit internal-control weaknesses over financial reporting have average loan spreads 28 basis points higher than firms that do not exhibit internal control weaknesses (Kim *et al.*, 2011).

Hypotheses Development: Cybersecurity Risk Disclosure's Quality and Cost of Debt

The literature discusses several measures of disclosure quality such as: 1) the number of words, 2) readability complexity, and 3) litigious language. Longer documents are used as a device to obscure negative news (Conway *et al.*, 2015). Longer documents can discourage recipients from reading the entire document, since it requires more information-processing capability (Jackson *et al.*, 2019; Loughran and McDonald, 2014). Management may attempt to hide bad news from stakeholders by hiding it in lengthier documents. "When the word size becomes larger, the more difficult the readability of the document becomes" (Jackson *et al.*, 2019). In a fraud context, Lee *et al.* (2013) find that fraudulent companies increase the number of words. With the increase in the number of words being perceived as an obfuscation technique, Calderon and Gao (2021) find a positive association between the number of words and audit fees, as auditors perceive a higher audit risk

based on the audit risk assessment. Similarly, the association of cost of debt and general disclosures' number of words has been analyzed in prior research. Fang-Klingler (2019) analyzes the readability of the annual reports in general. The author finds that reports with higher number of words are associated with higher cost of debt. Further, Chen *et al*. (2015) suggest that 10-K reports with higher number of words are associated with higher cost of debt and cost of equity. Neither of those two studies focuses on cybersecurity risk or its disclosures.

Since the number of words is considered a way to obscure bad news and deflect the reader's focus, we hypothesize the following:

H1: There is a positive association between the number of words in cybersecurity risk disclosure and cost of debt.

Another disclosure-quality measure is its readability. The readability of companies' disclosures is related to the ease with which a reader can understand the written text. The less readable a financial communication is, the more time and effort users must dedicate to decipher the relevant information, thereby making interpretation more difficult (Bloomfield, 2002). Difficult-to-read financial communication is either the result of management's inability to communicate clearly or its intentional acts to muddy the information (Bonsall and Miller, 2017). According to Li *et al.* (2018), management might obfuscate financial communications to hide its deficient performance. Bonsall and Miller (2017) examine financial disclosure readability on bond market outcomes. They find that less readable *financial* disclosures lead to lower bond ratings and consequently higher cost of debt. Less readable disclosures reduce investor confidence in the information, thereby affecting future judgments and decisions (Rennekamp, 2012). Difficult-to-read annual reports dissuade investors from evaluating information, thereby reducing stock-trading activity (Rjiba *et al.*, 2021).

Prior literature shows that higher readability complexity of disclosures leads to less confidence in disclosures and deters users from evaluating firms properly. Accordingly, we hypothesize:

H2: There is a positive association between readability difficulty of cybersecurity risk disclosure and cost of debt.

Other studies have considered the litigious language as a measure for general disclosure quality. Litigious words, which reflect a proclivity for legal contest, are significantly linked to lawsuits (Loughran and McDonald, 2014). When cybersecurity breach incidents occur, there is a significant increase in the use of litigious language in the disclosure of insurance risks (Gao *et al.*, 2020). When firms that face high cybersecurity risk fail to alert their investors in advance and then experience an actual cybersecurity incident, the firms may be exposed to lawsuits. Accordingly, management is likely to disclose cybersecurity risk, if it believes in a high likelihood of a future cybersecurity breach with a significant potential impact (Li *et al.*, 2018).

The SEC encourages firms to disclose information that does not contain legalistic language that is difficult for the readers to understand (SEC, 1998). Prior studies have analyzed the impact of litigious language in disclosures. Calderon and Gao (2021) suggest that difficult-to-read cybersecurity risk disclosures with more litigious language are associated with higher audit fees. Similarly, Malik *et al.* (2021) analyze the litigious tone in the 10-K reports of listed firms in the U.S. They find that reports with higher litigious tones are associated with higher audit fees. Furthermore, the authors discuss that auditors have less confidence in 10-K reports that include a litigious tone from high-risk clients. They conclude that litigious language reduces the credibility of disclosures. Bonsall and Miller (2017) find that narrative disclosures that are difficult to read due to higher legal terms tend to increase cost of debt. Also, they find that litigious language is associated with less favorable bond ratings. Accordingly, we hypothesize the following:

H3: There is a positive association between litigious language in cybersecurity risk disclosure and cost of debt.

III. Research Design

Sample Selection

Our sample is an intersection of data from Gao *et al.* (2020) for the disclosures and the Compustat database for the financial data. The raw data set was subject to data preprocessing. Data screening is a crucial step before running the further analysis (Hair *et.al.*, 2019). First, variables with heavy skewness around mean values are winsorized at 1% of the lower and upper tails of the data set by replacing the extreme values with their winsorized counterparts. Second, possible outliers were identified and removed from the research sample by using the minimum covariance determinant (MCD) method (Verardi and Dehon, 2010), which can provide robustness for the Mahalanobis distance. The variables with significant missing values

listwise were eliminated from the research sample. Therefore, the final sample size is 421 observations from 2010 to 2018. Table 1 panel A presents the detailed sample distribution.

Table 1 panel B presents the active/inactive status marker. Specifically, 3.33% of the firm-year observations are in 2010, 6.18% are in 2011, 9.03% are in 2011, 10.45% are in 2013, 13.3% are in 2014, 13.78% are in 2015, 14.25% are in 2016, 14.96% are in 2017, and 14.73% are in 2018. Furthermore, 88.6% of the observations were active, while 11.4% were inactive.

Table 1: Sample Summary and Distribution Based on Year and Status

Panel A

Initial sample	698
(-) Listwise missing values	179
(-) Multivariate significant outliers	98
Final Sample	421

Panel B

Variable	Categories	Frequency	Percent
Year	2010	14	3.33
	2011	26	6.18
	2012	38	9.03
	2013	44	10.45
	2014	56	13.3
	2015	58	13.78
	2016	60	14.25
	2017	63	14.96
	2018	62	14.73
	Total	*421*	*100*
Status marker	Active	373	88.6
	Inactive	48	11.4
	Total	*421*	*100*

To provide further details about the generalizability of the research sample and to determine the minimum sample size to perform the regression analyses in the forthcoming sections, a power analysis using G*Power is performed (Faul *et al.*, 2009). For the setting of the power analysis, the suggested (Faul *et al.*, 2009) parameters such as effect size f2(0.15), alpha error probability (α: 0.05), power (1-β error probability: 0.95), the number of predictors (15) are incorporated. According to the power analysis results, the minimum sample size of the proposed research models is 119. The current final sample size is 421 which is significantly larger than the obtained minimum sample size of 119. Therefore, the current sample size does not cause any potential biases.

Variables

Cybersecurity Risk Disclosure Variables

In the study, we use three cybersecurity risk disclosure variables. The first measure is *LNWORD*, that is the natural logarithm of the total number of words used to disclose cybersecurity risks in a company's 10-K. Electronic count is performed on the excerpts of text from the 10-K filing that contain cybersecurity disclosures. The second measure is the readability of cybersecurity risk disclosures, *READ.* Gao *et al.* (2020) use the readability consensus index computed through the Textstat Python package as a measure of the readability of cybersecurity risk disclosures. The higher the Readability Consensus index, the more difficult it is to read a passage of text. Indicators such as the number of words per sentence, the number of characters per word, and the number of syllables per word are the basis for computing most readability indices. The third measure is litigious language used in cybersecurity risk disclosures, *LITIGLANG*, that is computed by dividing the number of litigious words by the total number of words in the cybersecurity disclosures.

Cost of Debt

We measure a firm's cost of debt as the natural logarithm of its interest expense for the year divided by the average short-term and long-term debt during the same year, like Kim *et al*. (2011), Pittman and Fortin (2004), and Sanchez-Ballesta and Garcia-Meca (2011).

Empirical design

The detailed models used to test the three research hypotheses follow. The baseline research models utilize the GMM-based dynamic panel regression analysis. GMM examines the dynamic relationship that exists in the explanatory variables, that can alleviate the potential risk of omitted variable bias (Arellano and Bond, 1991). In the given three models, the functional relationship between cost of debt (dependent variable) and cybersecurity risk disclosure (independent variable) is formulated.

Model 1:

$$LNCOD_{it} = \alpha_1 LNCOD_{i,t-1} + \beta_1 LNWORD_{it} + \beta_2 LNTA_{it} + \beta_3 LEV_{it} + \beta_4 ROA_{it} + \beta_5 MTB_{it} + \beta_6 LOSS_{it} + \beta_7 TANG_{it} + \beta_8 SECTOR_{it} + \beta_9 SEC2011_{it} + \beta_{10} SEC2018_{it} + \beta_{11} RISK_{it} + \beta_{12} CYBERINC_{it} + \beta_{13} AUDITCHN_{it} + \beta_{14} EXECCHN_{it} + \beta_{15} BIGFOUR + \vartheta_i + \epsilon_{it}$$

Model 2:

$$LNCOD_{it} = \alpha_1 LNCOD_{i,t-1} + \beta_1 READ_{it} + \beta_2 LNTA_{it} + \beta_3 LEV_{it} + \beta_4 ROA_{it} + \beta_5 MTB_{it} + \beta_6 LOSS_{it} + \beta_7 TANG_{it} + \beta_8 SECTOR_{it} + \beta_9 SEC2011_{it} + \beta_{10} SEC2018_{it} + \beta_{11} RISK_{it} + \beta_{12} CYBERINC_{it} + \beta_{13} AUDITCHN_{it} + \beta_{14} EXECCHN_{it} + \beta_{15} BIGFOUR + \vartheta_i + \epsilon_{it}$$

Model 3:

$$LNCOD_{it} = \alpha_1 LNCOD_{i,t-1} + \beta_1 LITIGLANG_{it} + \beta_2 LNTA_{it} + \beta_3 LEV_{it} + \beta_4 ROA_{it} + \beta_5 MTB_{it} + \beta_6 LOSS_{it} + \beta_7 TANG_{it} + \beta_8 SECTOR_{it} + \beta_9 SEC2011_{it} + \beta_{10} SEC2018_{it} + \beta_{11} RISK_{it} + \beta_{12} CYBERINC_{it} + \beta_{13} AUDITCHN_{it} + \beta_{14} EXECCHN_{it} + \beta_{15} BIGFOUR + \vartheta_i + \epsilon_{it}$$

In the equations, the index "*i*" represents the firm as the panel variable, while the index "*t*" represents the year as the time variable. Furthermore, the error term is indicated by "$\vartheta_i + \epsilon_{it}$" where "$\vartheta_i$" is the panel-level effects and "ϵ_{it}" is the regular error term. The list of the research variables with a description is given in Appendix Table A1.

Table A1: List of Research Variables

Variable	Description
Dependent variable	
LNCOD	Natural logarithm of Cost of Debt (COD)
Independent testing variables	
LNWORD	Natural logarithm of the total number of words describing cybersecurity risks in a company's disclosure.
READ	The minimum level of education grade required to understand the text. The higher the Readability Consensus index the more difficult the index is to read.
LITIGLANG	The number of litigious words divided by the total number of words in cybersecurity disclosures
Independent control variables	
LNTA	Natural logarithm of total assets
LEV	Total liabilities divided by total assets
ROA	Ratio of earnings before tax to total assets
MTB	Market value of common shares divided by total book value of common shares
TANG	Percentage of intangible assets to total assets
RISK	Number of cybersecurity incidents each year

LOSS	1 if Net Income is negative; 0 if positive
SECTOR	1 if the firm belongs to one of the following three industry groups: consumer services, software and services, and Banking; 0 otherwise
SEC2011	1 if the disclosure is post- SEC 2011 Guidance (2011–2017); 0 otherwise (2007–2010).
SEC2018	1 if the disclosure is post- SEC Guidance (2018); 0 otherwise (2007–2017).
CYBERINC	1 if the disclosure has cyber incidents information; 0 otherwise.
AUDITCHN	1 if the company has a change of auditor during the year; 0 otherwise.
EXECCHN	1 if the company has a change of CEO, CFO, President, or Chairman of Board during the year; 0 otherwise.
BIGFOUR	1 if Big4 auditor is used, 0 otherwise

To support the three hypotheses, we expect each of the coefficients, *LNWORD*, *READ*, and *LITIGLANG*, to be positive and significant.

Following prior studies (e.g., Calderon and Gao (2021), Gao *et al.* (2020), and Pittman and Fortin (2004)), we include several control variables that affect the cost of debt and cybersecurity disclosure. *lnTA*, which is the natural logarithm of total assets, controls for size. Larger firms tend to use more words to disclose cybersecurity risks than smaller firms. *LEV*, leverage is total liabilities divided by total assets. Firms with higher leverage are more likely to have a higher cost of debt. *ROA*, return on assets, is the ratio of earnings before tax to total assets. This variable proxies for the ability of the company to invest in monitoring and disclosure of cybersecurity issues. *MTB*, market value of common shares divided by total book value of common shares, is a proxy for the firm's growth potential. That is, if market to book increases, cost of debt decreases. If creditors perceive growth positively for the firm, then a negative relationship exists with the cost of debt. *LOSS* is a dummy variable equal to one if the firm reports negative earnings. Firms with negative earnings are riskier and creditors will demand a higher interest rate on their loans. *TANG* is the percentage of intangible assets to total assets. A higher proportion of intangible assets may suggest more investment in software to combat cyber risks, which may decrease the cybersecurity risks. *SECTOR* is a control for industry. Its value is equal to one, if the firm belongs to one of the following three industry groups: consumer services, software and services, and banking; zero otherwise. *SEC2011* and *SEC2018*, are dummy variables that equal to one if the disclosure is post-2011 and -2018, respectively, zero otherwise. Companies responded to both the SEC 2011 and 2018 guidance by increasing the numbers of words in their cybersecurity risk disclosures. *RISK*, risk index is the number of cybersecurity incidents each year in the U.S. It measures the threat level of cyber attacks. Higher cybersecurity breaches are expected to increase the risks' disclosure. *CYBERINC* equals to one if the disclosure has cyber incident information, zero otherwise. This variable is an indicator of past risk and potential future cost in terms of litigation and lost market share associated with not disclosing cybersecurity incidents. *AUDITCHN*, auditor change proxies for the likelihood that a new auditor will urge management to disclose cybersecurity issues that could affect internal control and financial statements. *EXECCHN*, executive change serves as a proxy for the likelihood of new management perspectives on cybersecurity issues and the need for disclosure. Changes in the senior leadership of an organization (CEO, CFO, President, or Chairman of Board) can trigger changes in corporate governance mechanisms and impact the extent of disclosures in annual SEC filings (Elzahar and Hussainey, 2012; Ettredge *et al.*, 2011). *BIGFOUR* is a dummy variable that equals to one if the firm is audited by a Big4 audit firm, and zero otherwise.

The GMM-based dynamic model includes one lag of the *LNCOD* as a covariate as well as the unobserved panel-level fixed-effects to make the standard estimators consistent (Arellano and Bond, 1991). Also, this methodology utilizes the moment restrictions by improving Anderson and Hsiao's (1982)'s first-differenced approach which eliminates the potential bias caused by time-invariant unobserved heterogeneity. Accordingly, GMM-based dynamic panel regression generates consistent results in the presence of possible risk of endogeneity sources (Wintoki *et al.*, 2012).

There are various crucial reasons for our selection of the dynamic panel regression analysis. First, the GMM-type of dynamic panel regression is used where, as here, there are many panels with a few periods (Wooldridge, 2010). Second, the GMM-based dynamic panel is recommended since the independent testing variables (cybersecurity risk disclosure) are

persistent over time as they show unit roots in the panel data set (Kruiniger, 1999). Finally, it is utilized to alleviate the endogeneity concern (Naik and Padhi, 2015; Dutta and Roy, 2016)

The dynamic panel regression analysis is applied to test the proposed hypotheses. The estimators are established by first-differencing to remove the panel-level effects as well as by using instruments to establish the moment conditions. In the GMM-type of dynamic panel regression analysis, the lagged levels of the dependent variable, the predetermined variables, and endogenous variables are used to form the GMM-type instruments (Arellano and Bond, 1991; Holtz-Eakin *et al.*, 1988). Furthermore, Arellano-Bond robust variance-covariance estimator as well as Windmeijer (2005) robust estimators are reported for the standard errors to eliminate the heteroskedasticity issue.

IV. Results

Descriptive Statistics

The summary statistics of the research variables are included in Table 2. The numerical variables are summarized by average and standard deviation, while the categorical variables are summarized by using the frequency analysis. Namely, the results indicate that the mean value of *COD* is 62.32, *WORDS* is 337.94, *READ* is 19.30, and *LITIGLANG* is 0.02. Furthermore, 31.59% of the firm-year observations indicate the reporting of the net loss; 38.48% belong to one of the consumer services, software and services, and banking; and 75.06% are audited by a *BIGFOUR* auditor firm; 5.7% disclosure had cyber incidents information; 2.85% firms have a change of auditor during the year; and 68.88% firms changed CEO, CFO, President, or Chairman of Board during the year.

Table 2: Descriptive Statistics

Variable	N	Mean	Standard Deviation
COD	421	62.32	805.79
WORDS	421	337.94	243.21
READ	421	19.30	4.84
LITIGLANG	421	0.02	0.01
LNTA	421	13.68	2.52
LEV	421	0.34	0.81
ROA	421	-0.09	0.73
MTB	421	5.97	61.48
TANG	421	0.75	0.67
RISK	421	6.77	0.42

Variables	Categories	Frequency	Percent
LOSS	0	288	68.41
	1	133	31.59
	Total	*421*	*100.00*
BIGFOUR	0	105	24.94
	1	316	75.06
	Total	*421*	*100.00*
SECTOR	0	259	61.52
	1	162	38.48
	Total	*421*	*100.00*
SEC2011	0	14	3.33
	1	407	96.67
	Total	*421*	*100.00*
SEC2018	0	359	85.27
	1	62	14.73
	Total	*421*	*100.00*
CYBERINC	0	397	94.30
	1	24	5.70
	Total	*421*	*100.00*

AUDITCHN	0	409	97.15
	1	12	2.85
	Total	*421*	*100.00*
EXECCHN	0	131	31.12
	1	290	68.88
	Total	*421*	*100.00*

LOSS: 1 if Net Income is negative; 0 if positive
BIGFOUR: 1 if Big4 auditor is used, 0 otherwise
SECTOR: 1 if the firm belongs to one of the following three industry groups: consumer services, software and services, and Banking; 0 otherwise
SEC2011: 1 if the disclosure is post- SEC 2011 Guidance (2011–2017); 0 otherwise (2007–2010).
SEC2018: 1 if the disclosure is post- SEC Guidance (2018); 0 otherwise (2007–2017).
CYBERINC: 1 if the disclosure has cyber incidents information; 0 otherwise.
AUDITCHN: 1 if the company has a change of auditor during the year; 0 otherwise.
EXECCHN: 1 if the company has a change of CEO, CFO, President, or Chairman of Board during the year; 0 otherwise.

Correlation Analysis

The bivariate correlation among the research variables is examined. Pearson's correlation analysis is applied, and the results are provided in Table 3. The results reveal that *LITIGLANG* has a significant positive linear correlation with *LNCOD* ($p<0.05$) while *WORDS* and *READ* do not have a significant linear bivariate correlation with *LNCOD*.

Table 3: Correlation Analysis

..	Variables	V1	V2	V3	V4	V5	V6	V7	V8	V9
1	COD	1								
2	WORDS	0.046	1							
3	READ	0.083	0.044	1						
4	LITIGLANG	0.183*	0.111*	0.174*	1					
5	LNTA	-0.087	0.223*	0.168*	-0.142*	1				
6	LEV	-0.033	-0.046	-0.049	0.027	-0.213*	1			
7	ROA	-0.007	0.107*	0.03	-0.081	0.394*	-0.554*	1		
8	MTB	-0.005	-0.025	-0.051	-0.027	-0.026	0.003	0.009	1	
9	LOSS	0.065	-0.03	0.001	0.151*	-0.485*	0.078	-0.341*	0.039	1
10	TANG	-0.021	0.145*	0.05	-0.066	0.051	0.035	0.021	0.092	0.043
11	SECTOR	0.081	0.155*	-0.116*	0.311*	-0.265*	0.145*	-0.099*	-0.065	0.051
12	SEC2011	0.014	0.093	0.006	-0.009	0.06	0.021	-0.041	0.005	0.012
13	SEC2018	-0.032	0.267*	0.097*	0.066	0.008	0.107*	-0.022	0.042	-0.008
14	RISK	-0.073	0.267*	0.054	0.09	-0.019	0.085	-0.075	-0.016	0.089
15	CYBERINC	-0.019	0.114*	0.099*	0.153*	0.132*	-0.01	0.032	0.011	-0.057
16	AUDITCHN	-0.013	-0.012	0.001	0.036	-0.042	0.018	0.014	0.008	0.006
17	EXECCHN	-0.02	0.045	0.015	-0.028	0.281*	-0.009	-0.048	-0.018	-0.029
18	BIGFOUR	-0.116*	0.101*	0.059	-0.131*	0.648*	-0.144*	0.230*	-0.100*	-0.293*
..	Variables	V10	V11	V12	V13	V14	V15	V16	V17	V18
10	TANG	1								
11	SECTOR	-0.028	1							
12	SEC2011	0.057	-0.126*	1						
13	SEC2018	0.032	-0.067	0.077	1					
14	RISK	0.036	-0.108*	0.120*	0.354*	1				
15	CYBERINC	-0.08	-0.005	0.046	0.071	0.079	1			
16	AUDITCHN	-0.016	0.011	-0.048	-0.031	0.046	0.081	1		
17	EXECCHN	-0.014	0.004	0.076	-0.01	-0.043	0.01	-0.07	1	
18	BIGFOUR	-0.052	-0.199*	0.046	-0.024	-0.003	0.071	0	0.205*	1

**p<0.05*

Baseline Analysis

The proposed models are examined using the GMM-based dynamic panel regression analysis. The results along with two post-estimation analyses (Sargan test and Arellano-Bond test for zero autocorrelation) are shown in Table 4. The results of the Sargan test indicate that the overidentifying restrictions are valid (Null: Overidentifying restrictions are valid). Furthermore, the Arellano-Bond test for zero autocorrelation in first-differenced errors reveals that there is no significant risk of serial correlation (Null: No autocorrelation) in the first-differenced errors at order two.

The dependent variable is *LNCOD*, while the independent testing variables are *LNWORD*, *READ*, and *LITIGLANG*. According to the obtained results, the coefficient of *LNWORD* (0.47, p<0.01), *READ* (0.034, p<0.05), and *LITIGLANG* (20.9, p<0.05) are positive and significant. These results support the three hypotheses. Thus, the independent testing variables have a significant impact on *LNCOD*; this impact implies that as firms disclose more cybersecurity risks in the 10-K reports, the cost of debt increases for these firms.

The coefficients of *lnTA* and *LEV* are negative and significant. Although the coefficients of *SECTORS* are zero, removing this independent control variable did not change the significance and the direction of the *LNWORD*, *READ*, and *LITIGLANG*.

Table 4: GMM-Based Dynamic Panel Regression Analysis

	(1)	(2)	(3)
Independent variables	LNCOD	LNCOD	LNCOD
$LNCOD_{(t-1)}$	0.066	0.095	0.085
	(1.11)	(1.60)	(1.44)
LNWORD	**0.47*****		
	(3.11)		
READ		**0.034****	
		(2.34)	
LITIGLANG			**20.9****
			(2.09)
LNTA	-0.91***	-0.95***	-0.92***
	(-4.06)	(-4.17)	(-4.13)
LEV	-0.15**	-0.16**	-0.17**
	(-2.19)	(-2.27)	(-2.36)
ROA	0.24*	0.26*	0.26*
	(1.73)	(1.83)	(1.85)
MTB	-0.00013	0.00010	-0.00011
	(-0.17)	(0.13)	(-0.15)
LOSS	-0.20	-0.23	-0.19
	(-1.24)	(-1.45)	(-1.21)
TANG	0.0077	0.056	0.075
	(0.03)	(0.22)	(0.30)
SECTOR	0.00	0.00	0.00
	(.)	(.)	(.)
SEC2011	-0.099	0.20	0.089
	(-0.37)	(0.75)	(0.34)
SEC2018	-0.0098	0.061	0.068
	(-0.07)	(0.47)	(0.53)
RISK	-0.18	0.054	0.0042
	(-1.26)	(0.44)	(0.03)
CYBERINC	-0.19	0.16	0.23
	(-0.31)	(0.27)	(0.40)
AUDITCHN	-0.084	-0.092	-0.14
	(-0.31)	(-0.33)	(-0.50)
EXECCHN	0.15	0.15	0.17

	(1.29)	(1.22)	(1.41)
BIGFOUR	-0.37	-0.15	-0.15
	(-0.76)	(-0.30)	(-0.31)
Constant	8.96***	9.51***	9.85***
	(2.86)	(3.00)	(3.15)
Sargan test stat.	56.94	58.44	53.33
AR (1)	-1.64	-1.64	-1.68
AR (2)	0.59	0.49	0.76
N	338	338	338
χ^2-Stat.	38.64***	33.19***	33.44***

t statistics in parentheses
** p < 0.10, ** p < 0.05, *** p < 0.01*

Robustness

Multiple further analyses are performed in this section to examine the robustness of the baseline analysis. First, Arellano-Bover/Blundell-Bond dynamic panel regression analysis is used for the baseline model. The results are provided in Table 5. Accordingly, the results show that *LNWORDS* (0.97, p<0.05), *READ* (0.057, p<0.01), and *LITIGLANG* (60.9, p<0.05) have a significant positive relationship with *LNCOD*, also supporting the three hypotheses.

Table 5: Arellano-Bover/Blundell-Bond Dynamic Panel Regression

	(1)	(2)	(3)
Independent variables	LNCOD	LNCOD	LNCOD
$LNCOD_{(t-1)}$	0.20	0.26***	0.20
	(1.56)	(5.29)	(1.59)
LNWORD	**0.97****		
	(2.17)		
READ		**0.057*****	
		(3.55)	
LITIGLANG			**60.9****
			(1.99)
LNTA	-0.21	-0.15	-0.20
	(-0.90)	(-1.15)	(-0.81)
LEV	-0.20**	-0.21***	-0.21**
	(-2.46)	(-2.63)	(-2.42)
ROA	0.17	0.21	0.22
	(1.45)	(1.38)	(1.61)
MTB	-0.00011	0.00028	-0.000042
	(-0.39)	(0.33)	(-0.15)
LOSS	-0.054	-0.13	-0.076
	(-0.32)	(-0.74)	(-0.44)
TANG	0.20	0.40	0.43
	(0.64)	(1.58)	(1.17)
SECTOR	3.86*	4.22***	3.70*
	(1.73)	(6.09)	(1.71)
SEC2011	-0.0039	0.60**	0.42
	(-0.01)	(2.11)	(0.87)
SEC2018	-0.12	0.021	-0.0070
	(-0.90)	(0.15)	(-0.06)
RISK	-0.43*	0.036	-0.084
	(-1.87)	(0.26)	(-0.58)
CYBERINC	-2.22*	-1.57**	-1.19
	(-1.68)	(-2.55)	(-1.26)
AUDITCHN	-0.37	-0.40	-0.52

	(-0.89)	(-1.31)	(-1.19)
EXECCHN	0.20	0.20	0.24
	(1.27)	(1.52)	(1.49)
BIGFOUR	-1.21	-0.97*	-0.66
	(-1.23)	(-1.96)	(-0.79)
Constant	-2.32	-2.91	-1.50
	(-0.55)	(-1.57)	(-0.34)
N	412	412	412
χ^2-Stat.	81.32***	276.19***	67.90***

t statistics in parentheses
* $p < 0.10$, ** $p < 0.05$, *** $p < 0.01$

Second, the baseline research models are subject to an alternative analysis approach. Toward this objective, the research models are subject to further analysis using instrumental variable regression analysis for panel data with two-stage least squares (2SLS) generalizations of panel data approach. In the analysis, instrumental variable regression analysis for panel date with G2SLS estimator (Balestra and Varadharajan-Krishnakumar, 1987) is used. The one-year lag of the independent testing variables is used as the instrumental variables, which can be correlated with the endogenous variables, but cannot be correlated with the error term (Wooldridge, 2010; Godos-Díez *et al.*, 2018). The risk of endogeneity, as well as the omitted variable bias, can be controlled by using the 2SLS methodology (Angrist and Krueger, 2001).

The results are provided in Table 6. According to the obtained results, the coefficients of *LNWORD* (0.37, p<0.01), *READ* (0.052, p<0.10), and *LITIGLANG* (59.8, p<0.05) are positive and significant.

Table 6: Instrumental Variable Panel Regression Analysis

	(1)	(2)	(3)
Independent variables	LNCOD	LNCOD	LNCOD
LNWORD	**0.37*** **		
	(2.94)		
READ		**0.052***	
		(1.83)	
LITIGLANG			**59.8** **
			(2.07)
LNTA	-0.33***	-0.32***	-0.23***
	(-4.39)	(-4.20)	(-3.33)
LEV	-0.11	-0.11	-0.12
	(-1.55)	(-1.60)	(-1.42)
ROA	0.016	0.024	0.0025
	(0.14)	(0.21)	(0.02)
MTB	-0.00021	0.00019	-0.00026
	(-0.27)	(0.24)	(-0.29)
LOSS	-0.12	-0.14	-0.081
	(-0.84)	(-0.91)	(-0.46)
TANG	-0.11	-0.098	-0.0080
	(-0.69)	(-0.60)	(-0.05)
SECTOR	-0.22	-0.020	-0.35
	(-0.61)	(-0.05)	(-1.05)
SEC2011	-0.72***	-0.48*	-0.51
	(-2.65)	(-1.74)	(-1.58)
SEC2018	-0.017	0.026	-0.045
	(-0.12)	(0.18)	(-0.26)
RISK	-0.32**	-0.18	-0.27*
	(-2.32)	(-1.36)	(-1.68)
CYBERINC	-0.060	0.022	-0.088
	(-0.14)	(0.05)	(-0.21)

AUDITCHN	0.025	0.070	-0.000011
	(0.09)	(0.24)	(-0.00)
EXECCHN	0.10	0.088	0.077
	(0.83)	(0.71)	(0.53)
BIGFOUR	-0.049	0.041	-0.022
	(-0.16)	(0.13)	(-0.07)
Constant	2.97**	2.57*	1.85
	(2.30)	(1.88)	(1.32)
N	368	368	368
χ^2-Stat.	42.97***	36.37***	36.07***

t statistics in parentheses
* $p < 0.10$, ** $p < 0.05$, *** $p < 0.01$
The one-year lag of the testing variables is used as the instrumental variables

Third, the one-year lags of the independent testing variables of interest are used in the baseline result models to alleviate any potential endogeneity concerns by eliminating the correlation between the explanatory variables and the error term (Lehoucq and Perez-Linan, 2014). We alleviate any potential threats of causal identification without the need of any other data set other than the current research sample (Bellemare *et al.*, 2017), and address the causal inference (Reed, 2014), and mitigate the potential risk of reverse causality (Steinberg and Malhotra, 2014). The formulation of the proposed model is represented in equation (1) below.

$$y_{it} = \beta_0 + \beta_1 y_{i(t-1)} + \beta_2 X_{1i(t-1)} + \beta_3 X_{2i(t-1)} + v_i + \epsilon_{it} \quad i = 1, \ldots, N \text{ and } t = 1, \ldots, T_i. \qquad (1)$$

In equation (1), the *LNCOD* is the dependent variable denoted by the "y_{it}" term, $LNWORD_{(t-1)}$, $READ_{(t-1)}$, and $LITIGLANG_{(t-1)}$ are the one-year lag of the testing variables of interest denoted by the "$X_{1i(t-1)}$" term while the control variables are denoted by the "$X_{2i(t-1)}$" term. The proposed model is subject to the GMM-based dynamic panel regression analysis (Table 7). The results are consistent with the initial analysis results where the coefficients of $LNWORD_{(t-1)}$, $READ_{(t-1)}$, and $LITIGLANG_{(t-1)}$ are significant and positive.

Table 7: Lag of Testing Variables Using GMM-Based Dynamic Panel Regression Analysis

	(1)	(2)	(3)
Independent variables	LNCOD	LNCOD	LNCOD
LNCOD (t-1)	0.043***	0.035***	0.053***
	(10.93)	(8.96)	(12.39)
LNWORD(t-1)	**0.084*** **		
	(4.26)		
READ(t-1)		**0.027*** **	
		(9.00)	
LITIGLANG(t-1)			**22.5*** **
			(6.85)
LNTA	-0.95***	-0.88***	-1.08***
	(-19.51)	(-22.02)	(-17.09)
LEV	-0.12***	-0.11***	-0.12***
	(-3.87)	(-3.49)	(-3.98)
ROA	0.24***	0.22***	0.26***
	(11.60)	(10.44)	(14.07)
MTB	0.000095	-0.00023**	0.000088
	(0.79)	(-2.42)	(0.63)
LOSS	-0.18***	-0.16***	-0.13***
	(-7.83)	(-7.43)	(-4.97)
TANG	-0.040	-0.014	-0.066
	(-0.81)	(-0.29)	(-1.26)
SECTOR	0.00	0.00	0.00
	(.)	(.)	(.)

SEC2011	-0.13**	-0.16**	-0.11**
	(-2.44)	(-2.46)	(-2.33)
SEC2018	0.080***	0.093***	0.13***
	(4.26)	(6.22)	(5.28)
RISK	-0.036	0.013	0.052**
	(-1.45)	(0.43)	(2.06)
CYBERINC	0.17***	0.096	0.053
	(2.81)	(1.33)	(0.70)
AUDITCHN	-0.16***	-0.14***	-0.12***
	(-9.37)	(-6.55)	(-5.99)
EXECCHN	0.14***	0.13***	0.16***
	(9.49)	(10.21)	(10.51)
BIGFOUR	-0.36***	-0.30***	-0.46***
	(-9.17)	(-6.34)	(-9.85)
Constant	11.0***	9.60***	13.3***
	(17.96)	(16.82)	(14.75)
Sargan test stat.	47.10	44.04	42.76
AR (1)	-1.59	-1.63	-1.55
AR (2)	0.87	0.88	0.88
χ^2-Stat.	36996.48***	78633.17***	49724.77***

t statistics in parentheses
* $p < 0.10$, ** $p < 0.05$, *** $p < 0.01$

Finally, the change-on-change (difference) model approach is utilized to test the research hypotheses. The change model can alleviate any potential omitted variable bias (Tsang, Xie, Xin, 2019). The formulation of the proposed model is presented in equation (2) below.

$$\Delta y_{it} = \beta_0 + \beta_1 \Delta y_{i(t-1)} + \beta_2 \Delta X_{1i(t-1)} + \beta_3 \Delta X_{2i(t-1)} + v_i + \epsilon_{it} \quad i = 1, \ldots, N \text{ and } t = 1, \ldots, T_i. \qquad (2)$$

The changes in the variables from t-1 to t are denoted by "$\Delta X = X_t - X_{t-1}$". In equation (2), Δ*LNCOD* is the dependent variable denoted by the "Δy_{it}" term. Also, Δ*LNWORD*, Δ*READ*, and Δ*LITIGLANG* are the variables of interest denoted by the "$\Delta X_{1i(t-1)}$" term while the independent control variables are represented by the "$\Delta X_{2i(t-1)}$" term. The analysis results are reported in Table 8. The results show that the coefficients of Δ*LNWORD*, Δ*READ*, and Δ*LITIGLANG* are significant and positive which are compatible with the baseline analysis results.

Table 8: Change Model Approach Using GMM-Based Dynamic Panel Regression Analysis

	(1)	(2)	(3)
Independent variables	ΔLNCOD	ΔLNCOD	ΔLNCOD
$\Delta LNCOD_{(t-1)}$	-0.25***	-0.24***	-0.26***
	(-79.89)	(-55.78)	(-37.27)
ΔLNWORD	**0.28*** **		
	(7.87)		
ΔREAD		**0.0071*** **	
		(5.72)	
ΔLITIGLANG			**36.6*** **
			(14.85)
ΔLNTA	-0.81***	-0.77***	-0.80***
	(-9.41)	(-11.54)	(-8.07)
ΔLEV	-0.21***	-0.19***	-0.19***
	(-4.22)	(-4.18)	(-4.08)
ΔROA	0.26***	0.24***	0.24***
	(14.80)	(15.41)	(12.76)
ΔMTB	0.00021	0.00021*	0.00012
	(1.64)	(1.68)	(0.75)

ΔLOSS	-0.12***	-0.13***	-0.088***
	(-5.37)	(-5.42)	(-3.30)
ΔTANG	-0.026	0.0091	-0.0022
	(-0.78)	(0.16)	(-0.03)
ΔSECTOR	0.00	0.00	0.00
	(.)	(.)	(.)
ΔSEC2011	-0.059**	0.012	0.00098
	(-2.05)	(0.32)	(0.02)
ΔSEC2018	-0.26***	-0.25***	-0.31***
	(-6.13)	(-7.59)	(-10.92)
ΔRISK	-0.36***	-0.33***	-0.31***
	(-6.83)	(-7.86)	(-7.56)
ΔCYBERINC	-0.16**	0.068	0.12
	(-2.46)	(1.06)	(1.58)
ΔAUDITCHN	-0.12***	-0.086**	-0.12***
	(-3.69)	(-2.54)	(-3.20)
ΔEXECCHN	0.12***	0.11***	0.16***
	(10.12)	(7.49)	(9.99)
ΔBIGFOUR	0.36***	0.41***	0.60***
	(3.10)	(3.45)	(3.19)
Constant	0.066***	0.097***	0.084***
	(3.60)	(5.50)	(5.37)
Sargan test stat.	43.90	45.67	46.44
AR (1)	-1.62	-1.63	-1.59
AR (2)	0.82	0.81	0.75
χ^2-Stat.	43398.28***	51696.55***	21744.14***

t statistics in parentheses
* $p < 0.10$, ** $p < 0.05$, *** $p < 0.01$
Δ: $X_t - X_{t-1}$

V. Conclusion

The expansion of digital-technology use has accentuated the importance of cybersecurity as a new risk-management factor. Cybersecurity is becoming one of the top priorities for executives and boards of directors due to potential negative impacts upon firm value and operations (Li *et al.*, 2018). By implementing appropriate countermeasures, such as cybersecurity prevention and detection controls, management can mitigate the likelihood or potential impact of a risk (Grove and Clouse, 2020).

Stakeholders, including investors, capital markets, and the country at large, depend on the security and reliability of information and communications systems. Accordingly, cybersecurity risks pose serious threats. Companies rely on digital technology not only to conduct their business operations, but also to engage with their customers, partners, and others. Vulnerabilities extend to investee companies, investors' accounts at financial-services firms, the markets through which they trade, and the infrastructure upon which they rely. All industries are affected (SEC, 2018).

Globally, average total data breach costs rose to $4.24 million for 2021 (Ponemon Institute, 2021). Firms that are victims of cyberattacks frequently suffer long-lasting economic and reputational losses (Haapamäki and Sihvonen, 2019). A firm's sales growth significantly declines for the three-year period following a cyberattack, particularly for large firms and those operating in the retail industry (Kamiya *et al.*, 2018).

Most of the prior literature has focused on cyber incidents. Haapamaki and Sihvonen (2019) categorize prior cybersecurity studies as follows: 1) Information sharing and cybersecurity, 2) Cybersecurity investments, 3) Internal audit, controls, and cybersecurity, 4) Disclosure of cybersecurity activities, and 5) Security threats and security breaches. Few articles analyzed cybersecurity risk disclosures. The studies that have focused on cybersecurity risk disclosure considered mainly the impact on investors (Bennett, 2015; Li *et al.*, 2018), association with control activities (Smith *et al.*, 2019), evolution of the cybersecurity risk disclosure (Gao *et al.*, 2020), impact of the risk disclosure quality on auditors' behavior

(Caldereon and Gao, 2021). Gao *et al*. (2020) and Calderon and Gao (2021) are the first study that analyze the cybersecurity disclosure quality. Our paper fills the gap in the literature by extending the impact of cybersecurity disclosure linguistic features on the debt market that is rarely studied in the literature.

Linguistic features of cybersecurity risk disclosures may affect the perception of audit risk, and thus affect audit pricing. "Auditors should not just assess the impact of an incident on a company's financial statements, but also evaluate the risks of cybersecurity, more broadly, even if such event has not yet happened" (Calderon and Gao, 2021). After violations of technical financial covenants, creditors impose additional costs on borrowers both in terms of higher interest rates and the addition of new covenants on subsequent loans (Sheneman, 2017).

This study uses the GMM-based dynamic panel regression analysis to test our model. Cybersecurity risk disclosure quality is proxied by the: (1) total number of words describing cybersecurity risks in a company's disclosure; (2) readability level of the disclosure; and (3) number of litigious words divided by the total number of words in cybersecurity disclosures. We find that as firms' disclosure quality on cybersecurity risks in the 10-K reports declines, the cost of debt increases for these firms.

This research contributes to the literature by assisting management, boards of directors, legislators, and regulators in their evaluation of cybersecurity risk disclosures and disclosure guidance. An unintended result of the SEC's publishing disclosure guidance, however, is that many firms make cybersecurity risk disclosures even though they do not face elevated cybersecurity risks. Additionally, the SEC does not want firms to use "generic" cybersecurity risk disclosures that could be applicable to any firm. Accordingly, the SEC may consider a guidance revision that encourages disclosure only by firms that face a higher level of cybersecurity risks.

In addition to the literature contribution, our article has direct implications for people and organizations. In the digital era, consumers avoid buying products from companies that have been affected by a cyber attack or vulnerable to potential ones (Ponemon Institute, 2021). Also, investors avoid investing in such vulnerable organizations. Thus, our paper gives direct implications for the users of cybersecurity disclosures informing them that companies with lower cybersecurity risk disclosure quality are faced with a higher debt cost that may impact their overall profitability and long-term sustainability. Also, our results inform organizations to improve their disclosure quality and be more transparent when it involves cybersecurity risk. Having a better disclosure quality decreases the cost of conducting business.

Although the study results are robust, a few limitations exist. The sample selected considered solely the U.S. firms as we focus on the U.S. debt market. Future research can consider the cybersecurity risk disclosure in other markets such as Canada, China, and Europe. Also, future research can investigate the determinants of cybersecurity risk disclosure by considering CIO characteristics, CEO characteristics, board and audit committee characteristics. The results will guide organizations on how to improve cybersecurity disclosures. Furthermore, a future study can consider the evolution of cybersecurity risk disclosure over the years and analyze how the evolution would have been impacted with or without cyber attacks.

References

Anderson, T. W., and Hsiao, C. (1982). Formulation and estimation of dynamic models using panel data. *Journal of Econometrics, 18(1),* 47–82.

Angrist, J and Krueger, A. (2001), Instrumental Variables and the Search for Identification: From Supply and Demand to Natural Experiments, *Journal of Economics Perspectives, 15(4),* 69–85.

Arellano, M., and S. Bond. (1991). Some tests of specification for panel data: Monte Carlo evidence and an application to employment equations. *Review of Economic Studies, 58,* 277–297.

Balestra, P., and J. Varadharajan-Krishnakumar. (1987). Full information estimations of a system of simultaneous equations with error component structure. *Econometric Theory* 3: 223–246.

Bellemare, M. F., Masaki, T., and Pepinsky, T. B. (2017). Lagged explanatory variables and the estimation of causal effect. *The Journal of Politics, 79(3),* 949–963.

Bennett, C. (2015). *SEC weighs cybersecurity disclosure rules*. The Hill.

Bloomfield, R. J. (2002). The incomplete revelation hypothesis and financial reporting. *Accounting Horizons, 16(3),* 233–243.

Bonsall, S. B., and Miller, B. P. (2017). The impact of narrative disclosure readability on bond ratings and the cost of debt. *Review of Accounting Studies, 22(2),* 608–643.

Calderon, T. G., and Gao, L. (2021). Cybersecurity risks disclosure and implied audit risks: Evidence from audit fees. *International Journal of Auditing, 25(1),* 24–39.

Capital One, 2019. Information on the Capital One Cyber Incident. Available at: https://www.capitalone.com/facts2019/.

Chen, P. F., He, S., Ma, Z., and Stice, D. (2016). The information role of audit opinions in debt contracting. *Journal of Accounting and Economics, 61(1),* 121–144.

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

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

Chokshi, N. (2019). Hackers are holding Baltimore hostage: How they struck and what's next. The New York Times. a

Clayton, J. (2018). Statement on cybersecurity interpretive guidance. Available at https://www.sec.gov/news/public-statement/statement-clayton-2018-02-21.

Conway, S., O'Keefe, P., and Hrasky, S. (2015). Legitimacy, accountability and impression management in NGOs: The Indian Ocean tsunami. *Accounting, Auditing and Accountability Journal, 28(7),* 1075–1098.

Deloitte. (2020). Cybersecurity and the role of internal audit. An urgent call to action. Available at: https://www2.deloitte.com/us/en/pages/risk/articles/cybersecurity-internal-audit-role.html.

Department of Justice, 2017. How to protect your networks from ransomware. Available at: https://www.justice.gov/criminal-ccips/file/872771/download.

Dichev, I. D., and Skinner, D. J. (2002). Large-sample evidence on the debt covenant hypothesis. *Journal of accounting research*, *40*(4), 1091–1123.

Dutta, N., and Roy, S. (2016). The interactive impact of press freedom and media reach on corruption. *Economic Modelling,* 58, 227–236.

Dyreng, S. D., Vashishtha, R., and Weber, J. (2017). Direct evidence on the informational properties of earnings in loan contracts. *Journal of Accounting Research, 55*(2), 371–406.

Elzahar, H., Hussainey, K. (2012). Determinants of narrative risk disclosures in UK interim reports. *Journal of Risk Finance, 13(2),* 133–147.

Ettredge, M., Johnstone, K., Stone, M., Wang, Q. (2011). The effects of firm size, corporate governance quality, and bad news on disclosure compliance. *Review of Accounting Studies, 16(4),* 866–889.

Fang-Klingler, J. (2019). Impact of readability on corporate bond market. *Journal of Risk and Financial Management*, *12*, 1–18.

Faul, F., Erdfelder, E., Buchner, A., and Lang, A.-G. (2009). Statistical power analyses using G*Power 3.1: Tests for correlation and regression analyses. *Behavior Research Methods*, *41*, 1149–1160.

Gansler, J. and Lucyshyn, W. (2005). Improving the security of financial management systems: what are we to do? *Journal of Accounting and Public Policy, 24(1),* 1–9.

Gao, L., Calderon, T. G., and Tang, F. (2020). Public companies' cybersecurity risk disclosures. *International Journal of Accounting Information Systems*, *38*. Advance online publication.

Godos-Díez, J. L., Cabeza-García, L., Alonso-Martínez, D., and Fernández-Gago, R. (2018). Factors influencing board of directors' decision-making process as determinants of CSR engagement. *Review of Managerial Science, 12(1),* 229–253.

Grove, H., and Clouse, M. (2020). Financial and non-financial fraud risk assessment. *Journal of Forensic and Investigative Accounting, 12*(3), 422–441.

Haapamäki, E., and Sihvonen, J. (2019). Cybersecurity in accounting research. *Managerial Auditing Journal, 34(7),* 808–834.

Hair Jr, J. F., Black, W. C., Babin, B. J., and Anderson, R. E. (2019). *Multivariate data analysis*. Cengage Learning.

Holtz-Eakin, D., W. K. Newey, and H. S. Rosen. (1988). Estimating vector autoregressions with panel data. *Econometrica, 56,* 1371–1395.

Jackson, S., Vanteeva, N., and Fearon, C. (2019). An investigation of the impact of data breach severity on the readability of mandatory data breach notification letters: Evidence from U.S firms. *Journal of the Association for Information Science and Technology*, *70*(11), 1277–1289.

Jiang, W., Legoria, J., Reichelt, K., and Walton, S. (2021). Firm Use of Cybersecurity Risk Disclosure. *Journal of Information Systems*. Advance online publication.

Kamiya, S., Kang, J. K., Kim, J., Milidonis, A., and Stulz, R. M. (2018). *What is the impact of successful cyberattacks on target firms?* (No. w24409). National Bureau of Economic Research.

Kim, J.B., Simunic, D. A., Stein, M. T., and Yi, C. H. (2011). Voluntary audits and the cost of debt capital for privately held firms: Korean evidence. *Contemporary Accounting Research*, *28*, 585–615.

Knight, F. H. (1921). *Risk, uncertainty, and profit* (Vol. 31). Houghton Mifflin.

Kroll. (2018, February 26). 91% of companies surveyed experienced a fraud incident in 2017, says Kroll Annual Global risk report. Available at: https://www.firstpost.com/business/91-of-companies-surveyed-experienced-a-fraud-incident-in-2017-says-kroll-annual-global-risk-report-4367789.html.

Kruiniger, H. (1999). *GMM Estimation of Dynamic Panel Data Models with Persistent Data*. London: Queen Mary and Westfield College Working Paper No. 428.

Larson, S. (2017, December 20). The hacks that left us exposed in 2017. Available at https://money.cnn.com/2017/12/18/technology/biggest-cyberattacks-of-the-year/index.html.

Lee, C. C., Churyk, N. T., and Clinton, B. D. (2013). Validating early fraud prediction using narrative disclosures. *Journal of Forensic and Investigative Accounting*, *5(1),* 35–57.

Lehoucq, Fabrice, and Anibal P´erez-Li˜n´an (2014). Breaking Out of the Coup Trap: Political Competition and Military Coups in Latin America. *Comparative Political Studies* 47(8): 1105–1129.

Li, H., No, W. G., and Wang, T. (2018). SEC's cybersecurity disclosure guidance and disclosed cybersecurity risk factors. *International Journal of Accounting Information Systems*, *30*, 40–55.

Loughran, T., and McDonald, B. (2014). Measuring readability in financial disclosures. *Journal of Finance*, *69*(4), 1643–1671.

Malik, M. F., Shan, Y. G., and Tong, J. Y. (2021). Do auditors price litigious tone? *Accounting and Finance*. Advance online publication.

Morgan, S. (2018). Global Ransomware Damage Costs Predicted to Exceed $8 Billion In 2018. Available at: http://bit.ly/30Oc3VE.

Naik, P. K., and Padhi, P. (2015). On the linkage between stock market development and economic growth in emerging market economies: Dynamic panel evidence. *Review of Accounting and Finance*, 14(4), 363–381.

O'Connell, B. (2017, July 12). Companies that suffer a data breach see 42% slide in stock price. Available at: https://www.thestreet.com/story/14224071/1/companies-that-suffer-a-data-breach-see-42-slide-in-stock-price.html.

Pittman, J. A., and Fortin, S. (2004). Auditor choice and the cost of debt capital for newly public firms. *Journal of Accounting and Economics, 37*, 113–136.

Ponemon Institute. (2021). How much a data breach cost. https://www.ibm.com/security/data-breach.

Poulsen, K., McMillan, R., Evans, M. (2021). A hospital hit by hackers, a baby in distress: The case of the first alleged ransomware death. Available at: https://www.wsj.com/articles/ransomware-hackers-hospital-first-alleged-death-11633008116

Reed, W. Robert (2014). A Note on the Practice of Lagging Variables to Avoid Simultaneity. *Working Paper*, University of Canterbury.

Rennekamp, K. (2012). Processing fluency and investors' reactions to disclosure readability. *Journal of Accounting Research, 50(5),* 1319–1354.

Rjiba, H., Saadi, S., Boubaker, S., and Ding, X. S. (2021). Annual report readability and the cost of equity capital. *Journal of Corporate Finance, 67*. Advance online publication.

Sanchez-Ballesta, J. P., and Garcia-Meca, E. (2011). Ownership structure and the cost of debt. *European Accounting Review, 20*, 389–416.

Satter, R. (2021). Up to 1,500 businesses affected by ransomware attack, U.S. firm's CEO says. Available at: https://www.reuters.com/technology/hackers-demand-70-million-liberate-data-held-by-companies-hit-mass-cyberattack-2021-07-05/.

Securities and Exchange Commission (SEC). 1998. A plain English handbook: How to create clear SEC disclosure. Available at: https://www.sec.gov/pdf/hanbook.pdf.

Securities and Exchange Commission (SEC). 2011a. CF disclosure. Available at: https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

Securities and Exchange Commission (SEC). 2011b. How to read a 10-K/10-Q. Available at: https://www.sec.gov/fast-answers/answersreada10khtm.html.

Securities and Exchange Commission (SEC). 2018. Commission statement and guidance on public company cybersecurity disclosures. Available at: https://www.sec.gov/rules/interp/2018/33-10459.pdf.

Sheneman, A. (2017). Cybersecurity risk and the cost of debt. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3406217.

SIFMA, (2021). 2022 Capital Markets Outlook. Available at: https://www.sifma.org/2022-capital-markets-outlook/.

Smith, T. J., Higgs, J. L., and Pinsker, R. E. (2019). Do auditors price breach risk in their audit fees? *Journal of Information Systems, 33(2),* 177–204.

Spanos, G. and Angelis, L. (2016). The impact of information security events to the stock market: a systematic literature review. *Computers and Security, 58*, 216–229.

Stein, K. (2018). *Statement on commission statement and guidance on public company cybersecurity disclosures*. Available at https://www.sec.gov/news/public-state-ment/statement-stein-2018-02-21.

Steinberg, David A., and Krishna Malhotra (2014). The Effect of Authoritarian Regime Type on Exchange Rate Policy. *World Politics*, 66(3): 491–529.

Stiglitz, J. E., and Weiss, A. (1981). Credit rationing in markets with imperfect information. *The American Economic Review*, *71*(3), 393–410.

Swift, O., Colon, R., and Davis, K. (2020). The Impact of Cyber Breaches on the Content of Cybersecurity Disclosures. *Journal of Forensic and Investigative Accounting*, *12*(2), 197–212.

Tsang, A., Xie, F., and Xin, X. (2019). Foreign institutional investors and corporate voluntary disclosure around the world. *The Accounting Review*, 94(5), 319–348.

Verardi, V., and Dehon, C. (2010). Multivariate outlier detection in Stata. *The Stata Journal*, *10(2)*, 259–266.

Windmeijer, F. (2005). A finite sample correction for the variance of linear efficient two-step GMM estimators. *Journal of Econometrics, 126,* 25–51.

Wintoki, M. B., Linck, J. S. and Netter, J. M. (2012). Endogeneity and the dynamics of internal corporate governance. *Journal of Financial Economics, (105)3,* 581–606.

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