Market Reaction to Cyber Strategy Disclosure: Word Embedding Derived Approach

Rui Cao
University of British Columbia
rui.cao@sauder.ubc.ca

Özüm Kafaee
University of British Columbia
ozum.kafaee@ubc.ca

Arslan Aziz
University of British Columbia
arslan.aziz@sauder.ubc.ca

Hasan Cavusoglu
University of British Columbia
cavusoglu@sauder.ubc.ca

Abstract

In this study, we use a semi-supervised natural language processing (NLP) methodology to assess cybersecurity strategy of firms based on their 10-K filings. Adapted from the Cybersecurity Framework developed by the National Institute of Standards and Technology (NIST), five distinct cybersecurity strategies, namely identification, protection, detection, response, and recovery, are measured annually. We find evidence that cybersecurity identification strategy is positively and significantly associated with firm market value. For those firms experienced a cyberattack in the past, disclosing cybersecurity protection strategy is not positively assessed by the market. This paper makes contribution to the literature on cybersecurity by identifying the cyber strategies disclosed in 10-K reports using textual analysis, which can be used in future cyber studies. We further show empirical evidence of how market reacts to different strategies, which have valuable implications for industry as to how to better manage cyber risk.

Keywords: Cybersecurity Strategy, Disclosure, cyberattacks

1. Introduction

A firm's information assets and its associated technology infrastructure are highly valuable. Viewed as a critical enterprise asset, the firm's information is used to evaluate its overall business competency (White, 2019). Hence, corporations are greatly concern about any adverse event or malicious action that could potentially threaten the security of their information assets or jeopardize the smooth functioning of their IT systems, either led by accidental mistake or an intentional cyberattack.

In the past decade, the rapid advancement in technology seems to have been outpacing organizations' abilities to manage cyber risk, and organizations in every industry are facing a growing cyber risk gap (Accenture and Ponemon Institute, 2020). Risk Based Security (2020) reports that in 2019, there were 7,098 data breaches reported, exposing over 15.1 billion records, which is 284% higher compared to 2018 and 91% higher compared to 2017. As millions of employees around the world switched to remote working due to the COVID-19 pandemic crisis, it is more attractive for attackers to steal data or spread malware. The total number of cyberattack records in 2020 exceeded 37 billion, a 141% increase compared to 2019 (Risk Based Security, 2021).

Firms getting cyberattacks need to face litigation costs and reputation lost (Deloitte and Toronto Finance International, 2019). Consumers are also concerned about the negative impact from cyberattacks, especially following a series of high-profile data breaches such as the ones at Equifax, Target, and Marriot International that exposed a considerable amount of sensitive customer information (Swinhoe, 2020). How to better manage cyber risk and minimize the cost due to cyber incidents becomes a tough yet important issue for firms (Mithas et al., 2016).

Given that shareholders value firms' cybersecurity-related disclosures (Berkman et al., 2018; Gordon et al., 2010), we reason that the disclosures about the cybersecurity strategy can be valuable to investors. Those disclosures indicate a firm's capability to monitor and mitigate cyber risk. While researchers focus on business strategy, there has been a lack of research effort investigating the value of a firm's strategies in managing its cyber risks. In this paper, we seek to answer the following question:

URI: https://hdl.handle.net/10125/103371
978-0-9981331-6-4

How does the market value the disclosure of cybersecurity strategies in firms' 10-K reports?

To determine the cybersecurity strategies of a firm, we use the Framework for Improving Critical Infrastructure Cybersecurity (henceforth, the Cybersecurity Framework) outlined by NIST (2018). The Cybersecurity Framework is widely-adopted and an ideal source for us to delineate different cyber strategies. Tenable Network Security (March 2016) reports that 70% of organizations see the Cybersecurity Framework (NIST, 2018) as the best practice in cybersecurity risk management. We characterize cybersecurity strategies by the five core functions of the framework NIST (2018): *Identification*, *Protection*, *Detection*, *Response*, and *Recovery*.

We use a word-embedding derived approach to examine 10-K filings for the fiscal years between 1999 and 2018. We develop cybersecurity strategy scores for each firm-year observation and test our research question by regressing the cumulative abnormal return of the stock price recorded around the 10-K filing date on cybersecurity strategy scores, and the interaction of strategy scores with a variable measuring the cyberattack experience of the firm in the past. We control for firm-specific factors that prior research has shown to explain the firm market value.

We find that disclosing identification strategy can boost market reaction to 10-K filings. And after the cyberattack, disclosing protection cyber strategy can have a negative impact on market value, implying that stakeholders have lost confidence about how the companies are protecting the information system environment. Moreover, we also find that the market reacts positively to the detection cyber strategy disclosure after the cyberattack. Discussing detection strategy is a sign of more attention to detecting a cyberattack and can switch investors' impressions of the firm about cyber detection.

We contribute to the cybersecurity literature by providing a word-embedding based measurement for cyber strategy disclosure, as a tool to value a firm's cyber risk management. Instead of measuring cyber strategy as a whole, our cyber strategy measurement details the strategy into five functions, including identification, protection, detection, recovery and response. Each strategy corresponds to the company's risk management at different stages, so that shareholders can have a better picture about the company's cyber risk management. Additionally, we provide empirical evidence that the disclosures of different strategies are valued by the market differently. With consideration of how the market would react, our paper can be a guide for firms to devise their cyber security disclosures.

2. Background and Framework

Disclosures reflect a firm's internal information (Verrecchia, 1983). Early research on the motivation to disclose has shown that when there is no cost to disclose, full disclosure exists because investors believe that non-disclosing firms have the worst possible information (Grossman, 1981; Milgrom, 1981). If the internal information is positive in nature, the firm may disclose it to improve its valuation (Dye, 1985; Verrecchia, 1983). If the internal information is negative, the firm may still disclose risk factors to reduce litigation costs associated with possible future adverse events (Skinner, 1994).

In the context of cybersecurity disclosures, there is no definitive regulation regarding the actual content of disclosures. The passage of the Sarbanes-Oxley (SOX) Act in 2002 increased the needs for firms to invest more in information security. However, neither SOX nor the U.S. Securities and Exchange Commission (SEC) mandates firms to publicly disclose their information security activities. Hence, the voluntary disclosure of information security context can reflect firms' consideration of cybersecurity, and reveal worthwhile insights. There are two primary sections of 10-K filings where firms disclose risks and opportunities related to cybersecurity: Risk Factors (Item 1A), and Managements Discussion and Analysis of Financial Condition and Results of Operations (MD&A) (Item 7). Our study will focus on these 2 sections.

The Framework for Improving Critical Infrastructure Cybersecurity (i.e., the Cybersecurity Framework) (NIST, 2018) is the result of an ongoing collaborative effort involving industry, academia, and the U.S. government. The Cybersecurity Framework offers a risk-based approach to manage cybersecurity. It can be used to characterize a firm's cybersecurity strategy, and also to compare the cybersecurity strategies of a diverse set of firms.

Compared to other cybersecurity frameworks, such as the Organization of Standardization (ISO) 27001, ISO 27002, Federal Information Security Management Act (FISMA), and Service Organization Control (SOC) Type 2, the NIST cybersecurity framework has several advantages. This publicly accessible framework was developed to be used by organizations in any sector or community, hence the proposed principles and best practices to improve cyber security and resilience can be applied to all firms "regardless of size, degree of cybersecurity risk, or cybersecurity sophistication" (NIST, 2018). Moreover, it provides a common language for understanding, managing, and expressing cybersecurity risk for all stakeholders. It can be used

to help identify and prioritize actions for reducing cybersecurity risk, and it is a tool for aligning policy, business, and technological approaches to managing such a risk. It can be used to manage cybersecurity risk across entire organizations or it can be focused on the delivery of critical services within an organization (NIST, 2018). Lastly, by distinctly delineating 5 core functions, the framework provides a clear basis to identify different cyber strategies through textual analysis in this research.

Table 1. NIST Cybersecurity Framework Core functions.

Strategy	Description
Identification	Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities
Protection	Develop and implement appropriate safeguards to ensure delivery of critical services
Detection	Develop and implement appropriate activities to identify the occurrence of a cybersecurity event
Response	Develop and implement appropriate activities to take action regarding a detected cybersecurity incident
Recovery	Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident

The Cybersecurity Framework Core presents industry standards, guidelines, and practices across the organization from the executive level to the implementation/operations level. The five functions - Identify, Protect, Detect, Respond, Recover - provide a high-level, strategic view of the life cycle of an organization's management of cybersecurity risk. The five functions, which we refer to as *cybersecurity strategies* hereafter, are defined in Table 1.

The activities in the *Identification* strategy are aimed at understanding the business context, the resources, and the related cybersecurity risks. These activities enable an organization to focus and prioritize its cybersecurity efforts, and thus are fundamental for the effective use of the Cybersecurity Framework. The *Protection* strategy supports the ability to limit or contain the occurrence and impact of a potential cybersecurity event. The *Detection* strategy enables timely discovery of cybersecurity events. The *Response* strategy focuses on supporting the ability to minimize the impact of a cybersecurity incident. Finally, the primary goal of the *Recovery* strategy is to ensure the timely return of business operations to their normal state to reduce the impact of a cybersecurity incident (NIST, 2018).

3. Literature Review and Hypothesis Development

Cyberattacks are costly for firms due to direct out-of-pocket costs (e.g. the investigation and remediation costs, legal penalties, and regulatory penalties) and reputation loss (Kamiya et al., 2021). Past literature has shown extensively that cyberattacks negatively impact firms' market value (Acquisti et al., 2006; Amir et al., 2018; Cavusoglu et al., 2004; Garg et al., 2003; Gatzlaff and McCullough, 2010; Goel and Shawky, 2009; L. A. Gordon et al., 2011; Hinz et al., 2015; Modi et al., 2015; Morse et al., 2011; Yayla and Hu, 2011). Hence, a company's level of cyber risk is an important consideration for investors when making investment decisions (Ettredge and Richardson, 2003). However, there is little publicly available information regarding firms' information security management, which means that a company's efforts to minimize cyber risks are not directly observable by investors. Hence, investors face a significant degree of uncertainty regarding the nature, extent, and effectiveness of cybersecurity efforts.

Companies may be able to reduce uncertainty and be more attractive to investors by providing additional risk management disclosures (Deumes and Knechel, 2008; Easley and O'Hara, 2009; Jorgensen and Kirschenheiter, 2003). With the lack of publicly available information regarding firms' information security management, investors face a significant degree of uncertainty regarding the nature, extent, and effectiveness of cybersecurity efforts. Beyond the mere acknowledgment of cybersecurity risks, the particular characteristics of risk disclosures also have an impact on investors' assessment of the firm. Gordon et al. (2010) documents that, on average, voluntary information security disclosures in a company's 10-K are associated with an increase in stock price, but the effect is the greatest when the disclosures are related to *proactive* security measures. Investors place a higher value on the firm when managers emphasize their proactive activities when disclosing items about information security. This result is warranted as Wang et al. (2013) find that companies that disclose *actionable* information in their 10-K filings are less likely to experience cybersecurity incidents. Accordingly, we use the descriptions of strategies as outlined in table 1 and consider their

perception by investors when building our expectations regarding the individual impact of each cybersecurity strategy in the market.

The Identification strategy is at the core of the Cybersecurity Framework; it creates a base for all other strategies to build on. Unless a company can build an organizational understanding of cybersecurity, all other activities to manage cyber risk would lack the grounding required for successful results. Thus, we argue that investors would bake in a premium into equity prices for disclosures of the *Identification* strategy, and we hypothesize the following:

Hypothesis 1: *Disclosures of the Identification strategy of cybersecurity are positively associated with firm market value.*

For the impact of the Protection strategy, we consider the existence of successful past cyberattacks in the firm history. Extant literature suggests that the extent to which cybersecurity disclosures influence the attractiveness of an investment depends on whether investors think the disclosed information is reliable (Jennings, 1987; Mercer, 2004). Hirst et al. (2007) suggest that improving the perceived reliability of financial disclosure reduces stakeholder uncertainty about signals produced by managers. Similarly, Rennekamp (2012) finds a significant positive relationship between investors' perceptions of disclosure reliability and investment attractiveness. Although the studies cited earlier show a positive association between cyber risk disclosures and market value, indicating that investors believe the assertions made in 10-K reports are reliable, this may not be true in all circumstances. Specifically, investors may be less likely to think that management's cybersecurity disclosures are reliable when a company has experienced a prior cyberattack (Frank et al., 2019). Church and Schneider (2016) find that when investors are made aware that control has failed in the past, it triggers concerns about managers' competence, character, and ability to exercise adequate oversight. The more concerned investors are about management's trustworthiness and competence, the less likely they are to think that management's voluntary disclosures are reliable (Mercer, 2004).

With this in mind, we expect to see a positive relationship between Protection strategy disclosures and firm market value for firms. However, we expect this relationship to be negative for firms that experienced at least one successful cyberattack in the past. A successful cyberattack is a direct consequence of deficiencies in IT systems and services, signaling that although the company has disclosed a focus on Protection strategy, the firm may still fail to fulfill its implementation effectively. And such disclosure becomes unreliable in the presence of a past attack. Hence, we propose:

Hypothesis 2a: *Disclosures of the Protection strategy are associated positively with firm market value.*

Hypothesis 2b: *Disclosures of the Protection strategy are associated negatively with firm market value when a company has experienced at least one successful cyberattack in the past.*

Unlike preventive strategies, mitigative strategies (Detection, Response, Recovery) prepare the organization for the post-attack stage. The key objective is to effectively contain the damages following a cyberattack. Craighead et al. (2007) defines recovery and detection capacities as two important mitigation strategies to recover from supply chain disruptions. Studies found that recovery efforts (apology and compensation) can restore customer satisfaction, repurchase intention and word of mouth (Goode et al., 2017). Gwebu et al. (2018) finds that certain response strategies can help to mitigate the negative impact brought by a data breach. Hence, in a cybersecurity setting, actions taken by the company to ensure timely mitigation of the ramification of an attack is of utmost importance. Therefore, we expect investors to value disclosures of mitigative strategies positively on average. When the firm has past attacks, however, investors might perceive the risk of a cyberattack to be higher for such a firm, leading to a higher premium in equity prices for mitigative strategy disclosures. We hypothesize:

Hypothesis 3a: *Disclosures of the mitigative strategies are associated positively with firm market value.*

Hypothesis 3b: *Disclosures of the mitigative strategies are associated more positively with firm market value when a company has experienced at least one successful cyberattack in the past.*

4. Research Methodology

4.1. Measuring Cybersecurity Strategies

We use the breach dataset from Privacy Rights Clearinghouse (PRC), a repository for breach records, which have been extensively used in academic research. We then collect 10-K filings from the SEC EDGAR database, for the fiscal year from 2005 to 2018. As outlined earlier, we are primarily interested in the Risk Factors (item 1A) and MD&A (item 7) sections of each filing, so we consider the combination of these two sections as one document per firm-year observation. SEC did not mandate the Risk Factors section until 2005

when Regulation S-K Item 503(c) was issued, so our research focuses on the period after 2005.

The strategy scores are computed following the approach taken by Li et al. (2020) where the authors use a semi-supervised machine learning algorithm to measure corporate culture scores using earnings calls. Such an approach is useful because it does not require a considerable number of human-labeled training observations as in supervised methodologies, yet is still guided by humans (i.e., cybersecurity strategies and their seed words) so that the algorithm inductively gathers information about cybersecurity strategies from 10-K reports. In Figure 1, we provide a graphical representation of the whole process of measuring cybersecurity strategy scores using 10-K reports.

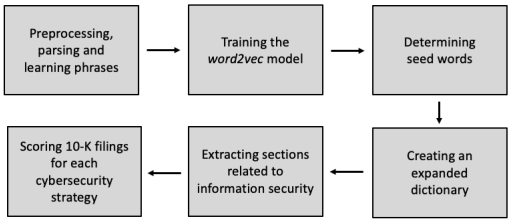

Figure 1. Summary of the process for measuring cybersecurity strategies

4.1.1. Preprocessing, Parsing, and Learning Phrases We use the *Stanford CoreNLP* package (Manning et al., 2014) to clean and parse the text into words. Then, Two- and three-word phrases are identified using the *phraser* module of the *gensim* library (Rehurek and Sojka, 2010). Lastly, we concatenate the phrases using the underscore symbol and treat them as a single word.

4.1.2. Training the *word2vec* Model The word embedding model we use in our study, *word2vec* (Mikolov et al., 2013), is a critical milestone in the Natural Language Processing (NLP) literature which enables analyses to go beyond the bag-of-words assumption, which ignores the order of words. *word2vec* uses a neural network to deeply parse the textual documents and efficiently learn dense and low-dimensional vectors to represent words and phrases. It is an effective way to quantify the semantics, rather than merely the syntactic, at the expression level (Li et al., 2020). We use the *gensim* library in Python to train the *word2vec* model. The dimension of word vectors is set to 300 and two words are defined as neighbors if they are no farther apart than 5 words in a sentence. We omit words that appear fewer than 5 times in the corpus. After training, each word in the corpus is denoted by a 300-dimensional vector that represents the meaning of that word.

4.1.3. Assigning Scores of Cybersecurity Strategy To develop the measure characterizing cyber strategy, we need to have a set of seed words for each of the five core risk management functions in the Cybersecurity Framework (NIST, 2018): *Identification*, *Protection*, *Detection*, *Response*, and *Recovery*. As explained earlier, these functions refer to distinct goals and activities for managing information security risk, thus providing a useful basis for identifying unique cybersecurity strategies. We examine the explanations of each of these functions in the Cybersecurity Framework document and determine units of meaning (i.e., seed words) for each strategy. If a particular seed word/phrase is not in the vocabulary of 10-K filings, it is then eliminated from the list (Li et al., 2020).

Generating an expanded, context-specific dictionary: As noted earlier, we get low-dimensional vectors as a result of the *word2vec* training process which enables quantifying the association between words or phrases by computing the cosine similarity between any two word-vectors (the higher cosine similarity between two vectors, the closer their association). Using this capability, we construct the expanded dictionary by associating a set of words or phrases in the documents to seed words defining each strategy. As a result, we get an expanded, context-specific dictionary to measure cybersecurity strategies. Specifically, we compute the average of the vectors of all the seed words for a particular strategy. We then compute the cosine similarity between each unique word in 10-K reports with this average vector. Instead of having a fixed amount of expanded words for each strategy (Li et al., 2020), we set a fixed similarity score threshold (0.4) and only keep the words whose similarity scores are above the threshold. As a result, each strategy has a different number of words in the expanded dictionary, where *protection* has 561 words, followed by *identification* with 132 words. *Recovery* has the least number of words of 21, indicating that there are not many $recovery$ related contents in the 10-K report. We apply the same strategy dictionaries to all data files, so the imbalance in the number of words will not lead to a bias of the strategy scores. We also manually go through the word dictionary to maintain high accuracy. If a word appears in dictionaries for multiple strategies, we choose the one with the highest cosine similarity.

Extracting Texts Related to Cybersecurity: The

MD&A and Risk Factors sections in the 10-K report typically contain discussions of various types of business risks and risk management. To get the scores related to cybersecurity strategies, we extract texts related to cyber risk so that our scores would not be contaminated by the discussions of other types of risks. Specifically, just like the seed words for each strategy, we create a list of seed words for information security following Gordon et al. (2010), enabling us to get an expanded dictionary to detect the discussions of cybersecurity in documents. Again, if a particular word or phrase does not appear in the corpus, it is not included in the seed words list for information security. We extract sentences that include one or more of the words or phrases included in the expanded dictionary for cybersecurity-related contexts. To sum up, the corpus that is used in our study, is the cybersecurity related sentences in 10-K reports item 1A and item 7.

Scoring Cybersecurity Strategies: After generating the strategy dictionary and extracting cybersecurity-related sentences, we measure each of the five cybersecurity strategies at the firm-year level. Following Loughran and McDonald (2011), we use the weighted count of the number of words associated with each value divided by the total number of words in the document where the weight is term frequency-inverse document frequency (tf-idf). Using tf-idf allows us to catch the level of importance of a word in a corpus, but not just the number of times that a word appears in a corpus. For example, a high identification tf-idf score in a 10-K filing indicates that the identification strategy takes an important place in the corpus and that the company focuses on identification to a greater extent. Across the data period, the yearly average scores for all five strategies increase over time. Protection strategy has the highest average tf-idf score every year, reaching 18.9 by 2018, while recovery strategy has the lowest yearly score, around 1.0 in 2018.

4.2. Sample

As clarified in section 4.1, our sample period ranges from 2005 to 2018. Cyberattack incidents were collected from Privacy Rights Clearinghouse (PRC). And we collected 100,029 10-K reports from the EDGAR database. After deleting 4,987 records that have neither of the two items, 95,042 reports remain. Recall that we only extract cybersecurity-related context, and 32,284 filings do not have such information. Finally, we calculated the cybersecurity strategy scores for the 62,758 corpora.

We collect financial data from Compustat and daily stock returns from CRSP, which are available on Wharton Research Data Services (WRDS), and we winsorize all continuous variables at the 1st and 99th percentiles to mitigate the impact of outliers in our analysis.

4.3. Research Design

The research model used in our study is a modified version of the model used by Gordon et al. (2010) to study the association between information security risk factors mentioned in annual reports and firm value. Our additions to this model are the inclusion of a variable measuring past cyberattack experience of the firm and the change of the dependent variable from stock price to cumulative abnormal return on the stock price. The control variables include *book value per share, earnings per share, size, return on asset (ROA), leverage* and *loss*. HBGary, Inc. (2013) indicate that nearly 80% of investors would not likely consider investing in firms with a history of cyberattacks, so to control for any differences in firm market value that might result from such attitude of investors, we include the prior attack variable as an indicator to see if a cyberattack happened anytime before the focal date of the 10-K filing. We follow Clarke et al. (2020) when using cumulative abnormal return (CAR) as a measurement to firm's equity value. CAR is calculated by

$$ARet_{i,t} = Ret_{i,t} - Ret_{m,t}$$

where $ARet_{i,t}$ is the abnormal return of the focal firm's primary ticker, $Ret_{i,t}$ is the actual return, $Ret_{m,t}$ is the return on the CRSP value-weighted index for firm i at time t with market m. In this study, we focus on 3 CAR windows: $[0, +1]$, $[0, +2]$, and $[0, +7]$, to account for 1, 2, and 7 trading days after time t, respectively. To improve interpretability in regression results, we take the natural logarithm of all strategy scores.

To investigate Hypothesis 1, 2a, and 3a, equation (1) is used to explain the association between post-event CAR and cyber strategy disclosures.

$$\begin{aligned} \text{CAR}_{i,[t,t+n]} = {} & \beta_0 \text{Constant}_{i,t} + \beta_1 \text{Identification}_{i,t} \\ & + \beta_2 \text{Protection}_{i,t} + \beta_3 \text{Detection}_{i,t} \\ & + \beta_4 \text{Response}_{i,t} + \beta_5 \text{Recovery}_{i,t} \\ & + \beta_6 \text{Prior Attack}_{i,t} + \text{Controls} \\ & + \text{Year dummies} + \text{Industry dummies} \\ & + \epsilon_{it} \end{aligned} \tag{1}$$

where $\text{CAR}_{i,[t,t+n]}$ denotes the cumulative abnormal return (CAR) for firm i around time window $[t, t +$

$n]$, where t is the 10-K filing date. $\text{Identification}_{i,t}$, $\text{Protection}_{i,t}$, $\text{Detection}_{i,t}$, $\text{Response}_{i,t}$, $\text{Recovery}_{i,t}$ denote the natural logarithm for 5 cybersecurity strategies of firm i's 10-K filed on date t. *Prior Attack*$_{i,t}$ equals to 1 if the firm i has experienced at least one cyberattack prior to filing date t, 0 otherwise. Controls are the financial variables shown on 10-K filed on date t. Hence, we want to account for market reaction to a 10-K report using the financial measures for the corresponding fiscal year.

$$\begin{aligned}\text{CAR}_{i,[t,t+n]} = {} & \beta_0 \text{Constant}_{i,t} + \beta_1 \text{Identification}_{i,t} \\ & + \beta_2 \text{Protection}_{i,t} + \beta_3 \text{Detection}_{i,t} \\ & + \beta_4 \text{Response}_{i,t} + \beta_5 \text{Recovery}_{i,t} \\ & + \beta_6 \text{Prior Attack}_{i,t} + \\ & + \beta_7 \text{Identification}_{i,t} * \text{Prior Attack}_{i,t} \\ & + \beta_8 \text{Protection}_{i,t} * \text{Prior Attack}_{i,t} + \\ & + \beta_9 \text{Detection}_{i,t} * \text{Prior Attack}_{i,t} + \\ & + \beta_{10} \text{Response}_{i,t} * \text{Prior Attack}_{i,t} + \\ & + \beta_{11} \text{Recovery}_{i,t} * \text{Prior Attack}_{i,t} + \\ & + \text{Controls} + \text{Year dummies} \\ & + \text{Industry dummies} + \epsilon_{it}\end{aligned} \tag{2}$$

We use equation (2) to test Hypothesis 2b and 3b. Interaction terms are included to test the moderating effect of having at least one successful cyberattack before the 10-K filing date. All other variables remain the same.

5. Results

Table 2 shows the estimations of models specified. In line with Hypothesis 1, the coefficients for Identification across all models are positive and significant, indicating that investors positively value the disclosure of the Identification strategy in the context of information security.

No evidence shows that discussing protection strategy can bring value to the firm, failing to reject the null hypothesis for hypothesis 2a. Columns 2, 4, and 6 test the moderating role of having a successful cyberattack before the 10-K filing date. The discussions of the Protection strategy are negatively and significantly associated with market value for firms that have experienced at least one cyberattack in the past, so Hypothesis 2b is supported. This result extends the literature focusing on the reliability of company disclosures. Our evidence suggests that investors perceive the management to be failing at protecting the firm from attacks and thus, penalizing the firm for the discussion of Protection strategy in their 10-K reports.

We do not find sufficient evidence to support Hypothesis 3a. In other words, there is no consistent evidence that investors value mitigative strategies positively or negatively as a whole. However, Hypothesis 3b is partially supported as the coefficient for Detection is positive and significant in all windows for breached companies, shown in columns 2, 4, and 6. And the effect size is the largest among all other strategies. The coefficients show that the disclosure of detection strategy by a firm that experienced a prior attack is associated with positive CARs around the report release date. Our results reveal that for firms that already had cyberattacks, discussing more detect strategies can increase their market value around the 10-K filing date. Discussing more detection-related content is a sign that the firm pays more attention to detecting cyber incidents, and our results show that such discussion makes investors perceive an attacked firm more favorably.

6. Contributions, limitations and conclusions

Our paper makes contributions to the literature on cybersecurity risk management. First, we study firms' information security activities in a strategy context using a widely-adopted industry framework - Framework for Improving Critical Infrastructure Cybersecurity (NIST, 2018). To the best of our knowledge, no previous studies have taken this approach and systematically investigated into the topic. Second, we believe that our analysis of 10-K disclosures is unique in cybersecurity content. Prior work about cybersecurity disclosures only consider a limited categories of cyber-related contexts by using keyword-detection method (Gordon et al., 2010; Wang et al., 2013). Our paper extends and complements earlier efforts by using the word embedding model (Mikolov et al., 2013) to measure corporate cybersecurity strategy that can be easily applied to a large sample of firms periodically. Finally, we show empirical evidence that different cybersecurity strategies have varying impacts on firm market value which is contingent on the prior breach experience of the firm.

A key insight from our results is that investors value disclosures of cybersecurity strategy in 10-K filings. As such, this study has implications for firms as they consider adopting preventive and/or mitigative strategies and communicating these decisions and activities to investors in markets with high levels of cybersecurity

Table 2. OLS regressions of CAR with various windows around disclosure date

	(1) CAR[0,1]	(2) CAR[0,1]	(3) CAR[0,2]	(4) CAR[0,2]	(5) CAR[0,7]	(6) CAR[0,7]
Identification	0.098***	0.100***	0.098***	0.099**	0.134**	0.140***
	(0.033)	(0.034)	(0.038)	(0.039)	(0.052)	(0.054)
Protection	0.006	0.015	0.036	0.046	0.049	0.060
	(0.030)	(0.031)	(0.035)	(0.036)	(0.049)	(0.050)
Detection	0.020	-0.002	0.010	-0.009	0.074	0.046
	(0.042)	(0.044)	(0.047)	(0.049)	(0.064)	(0.067)
Respond	-0.020	-0.021	-0.044	-0.047	-0.026	-0.034
	(0.032)	(0.033)	(0.037)	(0.038)	(0.051)	(0.053)
Recover	0.000	0.006	0.012	0.015	0.006	0.001
	(0.048)	(0.050)	(0.054)	(0.057)	(0.073)	(0.077)
Identification × Prior Attack		-0.044		-0.027		-0.145
		(0.118)		(0.125)		(0.172)
Protection × Prior Attack		-0.216*		-0.254*		-0.258
		(0.125)		(0.134)		(0.190)
Detection × Prior Attack		0.375***		0.329**		0.466**
		(0.140)		(0.153)		(0.206)
Response × Prior Attack		0.017		0.087		0.162
		(0.110)		(0.119)		(0.168)
Recovery × Prior Attack		-0.084		-0.050		0.071
		(0.149)		(0.160)		(0.218)
Prior Attack	-0.072	0.358	-0.074	0.359	-0.101	0.230
	(0.112)	(0.368)	(0.122)	(0.396)	(0.164)	(0.561)
Control	yes	yes	yes	yes	yes	yes
Industry FE	yes	yes	yes	yes	yes	yes
Year FE	yes	yes	yes	yes	yes	yes
Adj. R-squared	0.008	0.008	0.009	0.009	0.009	0.009
Obs.	35546	35546	35536	35536	35491	35491

Robust standard error is reported in parentheses. *, **, *** represent significance levels of 0.10, 0.05, and 0.01, respectively.

risk. Thus, this study not only answers an interesting and managerially relevant empirical research question but also provides directions for motivating a program of research to clarify and elaborate the findings through further theoretical or empirical work. We found that the market reacts positively to disclosure about identification strategy, indicating that stakeholders value the focus on organizational understanding of managing cybersecurity risk. We also provide evidence that protection strategy disclosure loses reliability after a cyberattack happened. And discussing detection-related contents after a cyberattack can reduce investors' uncertainty about the firm's cyber environment, thus increasing the market value around the filing release date.

We note the following limitations in our study. First, similar to other studies that use computation-intensive techniques, our study is a joint test of the appropriateness of the measure and our hypotheses. The empirical evidence's validity relies on our strategy measures' reliability. Second, 10-K filings provide a host of other information. Our inferences may be inappropriate if other information in the 10-K filings correlates with cybersecurity strategies despite our controls for firm characteristics. Finally, our empirical tests are primarily tests of association. For this reason, the causality may not be inferred.

References

Accenture, & Ponemon Institute. (2020). Ninth annual cost of cybercrime study [Available at https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf].

Acquisti, A., Friedman, A., & Telang, R. (2006). Is there a cost to privacy breaches? an event study. *Proceedings of the Twenty Seventh International Conference on Information Systems*, 94.

Amir, E., Levi, S., & Livne, T. (2018). Do firms underreport information on cyber-attacks? evidence from capital markets. *Review of Accounting Studies*, *23*(3), 1177–1206.

Berkman, H., Jona, J., Lee, G., & Soderstrom, N. (2018). Cybersecurity awareness and market valuations. *Journal of Accounting and Public Policy*, *37*(6), 508–526.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers. *International Journal of Electronic Commerce*, *9*(1), 70–104. https://doi.org/10.1080/10864415.2004.11044320

Church, B. K., & Schneider, A. (2016). The Impact of Section 302 and 404(b) Internal Control Disclosures on Prospective Investors' Judgments and Decisions: An Experimental Study. *International Journal of Auditing*, *20*(2), 175–185. https://doi.org/10.1111/ijau.12065

Clarke, J., Chen, H., Du, D., & Hu, Y. J. (2020). Fake news, investor attention, and market reaction. *Information Systems Research*, *32*(1), 35–52.

Craighead, C. W., Blackhurst, J., Rungtusanatham, M. J., & Handfield, R. B. (2007). The severity of supply chain disruptions: Design characteristics and mitigation capabilities. *Decision sciences*, *38*(1), 131–156.

Deloitte, & Toronto Finance International. (2019). The changing faces of cybersecurity - closing the cyber risk gap [Available at https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/risk/ca-cyber-talent-campaign-report-pov-aoda-en.PDF].

Deumes, R. W. J., & Knechel, W. R. (2008). Economic incentives for voluntary reporting on internal risk management and control systems. *Auditing : a journal of practice and theory*, *27*(1), 35–66.

Dye, R. A. (1985). Disclosure of nonproprietary information. *Journal of Accounting Research*, *23*(1), 123–145.

Easley, D., & O'Hara, M. (2009). Ambiguity and nonparticipation: The role of regulation. *The Review of Financial Studies*, *22*(5), 1817–1843.

Ettredge, M. L., & Richardson, V. J. (2003). Information transfer among internet firms: The case of hacker attacks. *The Journal of information systems*, *17*(2), 71–82.

Frank, M. L., Grenier, J. H., & Pyzoha, J. S. (2019). How Disclosing a Prior Cyberattack Influences the Efficacy of Cybersecurity Risk Management Reporting and Independent Assurance. *Journal of Information Systems*, *33*(3), 183–200. https://doi.org/10.2308/isys-52374

Garg, A., Curtis, J., & Halper, H. (2003). The financial impact of it security breaches: What do investors think? *Information Systems Security*, *12*(1), 22–33.

Gatzlaff, K. M., & McCullough, K. A. (2010). The effect of data breaches on shareholder wealth. *Risk Management and Insurance Review*, *13*(1), 61–83.

Goel, S., & Shawky, H. A. (2009). Estimating the market impact of security breach announcements on firm values. *Information Management*, *46*(7), 404–410.

Goode, S., Hoehle, H., Venkatesh, V., & Brown, S. A. (2017). User compensation as a data breach recovery action: An investigation of the sony playstation network breach. *MIS Quarterly*, *41*(3), 703–727.

Gordon, L. A., Loeb, M. P., & Zhou, L. (2011). The impact of information security breaches: Has there been a downward shift in costs? *Journal of Computer Security*, *19*(1), 33–56. https://doi.org/10.3233/JCS-2009-0398

Gordon, Loeb, & Sohail. (2010). Market Value of Voluntary Disclosures Concerning Information Security. *MIS Quarterly*, *34*(3), 567. https://doi.org/10.2307/25750692

Grossman, S. J. (1981). The informational role of warranties and private disclosure about product quality. *The Journal of law economics*, *24*(3), 461–483.

Gwebu, K. L., Wang, J., & Wang, L. (2018). The role of corporate reputation and crisis response strategies in data breach management. *Journal of Management Information Systems*, *35*(2), 683–714.

HBGary, Inc. (2013). Cybersecurity directly affects investor attitudes, new hbgary survey finds. [Available at https://www.prnewswire.com/news-releases/cybersecurity-directly-affects-investor-attitudes-new-hbgary-survey-finds-193105951.html].

Hinz, O., Nofer, M., Schiereck, D., & Trillig, J. (2015). The influence of data theft on the share prices and systematic risk of consumer electronics companies. *Information Management*, *52*(3), 337–347.

Hirst, D. E., Koonce, L., & Venkataraman, S. (2007). How disaggregation enhances the credibility of management earnings forecasts. *Journal of Accounting Research*, *45*(4), 811–837. https://doi.org/10.1111/j.1475-679X.2007.00252.x

Jennings, R. (1987). Unsystematic Security Price Movements, Management Earnings Forecasts, and Revisions in Consensus Analyst Earnings Forecasts. *Journal of Accounting Research*, *25*(1), 90. https://doi.org/10.2307/2491260

Jorgensen, B. N., & Kirschenheiter, M. T. (2003). Discretionary risk disclosures. *The Accounting Review*, *78*(2), 449–469.

Kamiya, S., Kang, J.-K., Kim, J., Milidonis, A., & René, M. S. (2021). Risk management, firm reputation, and the impact of successful cyberattacks on target firm. *Journal of Financial Economics*, *139*(3), 719–749. https://doi.org/10.1016/j.jfineco.2019.05.019

Li, K., Mai, F., Shen, R., & Yan, X. (2020). Measuring Corporate Culture Using Machine Learning. *The Review of Financial Studies*, *34*(7), 3265–3315. https://doi.org/10.1093/rfs/hhaa079

Loughran, T., & McDonald, B. (2011). When is a liability not a liability? textual analysis, dictionaries, and 10-ks. *The Journal of Finance*, *66*(1), 35–65.

Manning, C. D., Surdeanu, M., Bauer, J., Finkel, J. R., Bethard, S., & McClosky, D. (2014). The stanford corenlp natural language processing toolkit. *Proceedings of 52nd annual meeting of the association for computational linguistics: system demonstrations*, 55–60.

Mercer, M. (2004). How do investors assess the credibility of management disclosures? *Accounting Horizons*, *18*(3), 185–196. https://doi.org/10.2308/acch.2004.18.3.185

Mikolov, T., Sutskever, I., Chen, K., Corrado, G., & Dean, J. (2013). Distributed representations of words and phrases and their compositionality.

Milgrom, P. R. (1981). Good news and bad news: Representation theorems and applications. *The Bell journal of economics*, *12*(2), 380–391.

Mithas, S., Rust, R. T., & of Maryland, U. (2016). How information technology strategy and investments influence firm performance: Conjecture and empirical evidence. *MIS quarterly*, *40*(1), 223–245.

Modi, S. B., Wiles, M. A., & Mishra, S. (2015). Shareholder value implications of service failures in triads: The case of customer information security breaches. *Journal of Operations Management*, *35*(1), 21–39.

Morse, E. A., Raval, V., & Wingender, J. R. (2011). Market price effects of data security breaches. *Information Security Journal: A Global Perspective*, *20*(6), 263–273.

NIST. (2018). Framework for Improving Critical Infrastructure Cybersecurity Version 1.1. Retrieved April 30, 2020, from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Rehurek, R., & Sojka, P. (2010). Software framework for topic modelling with large corpora. *In Proceedings of the LREC 2010 workshop on new challenges for NLP frameworks*.

Rennekamp, K. (2012). Processing Fluency and Investors' Reactions to Disclosure Readability. *Journal of Accounting Research*, *50*(5), 1319–1354. https://doi.org/10.1111/j.1475-679X.2012.00460.x

Risk Based Security. (2020). 2019 year end report data breach quickview.

Risk Based Security. (2021). 2020 year end report data breach quickview.

Skinner, D. J. (1994). Why firms voluntarily disclose bad news. *Journal of Accounting Research*, *32*(1), 38–60.

Swinhoe, D. (2020). The 15 biggest data breaches of the 21st century [Available at https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html].

Tenable Network Security. (March 2016). Trends in security framework adoption: A survey of it and security professionals [Available at https://www.tenable.com/whitepapers/trends-in-security-framework-adoption].

Verrecchia, R. E. (1983). Discretionary disclosure. *Journal of Accounting and Economics*, *5*(1), 179–194.

Wang, T., Kannan, K. N., & Ulmer, J. R. (2013). The Association Between the Disclosure and the Realization of Information Security Risk Factors. *Information Systems Research*, *24*(2), 201–218. https://doi.org/10.1287/isre.1120.0437

White, A. (2019). Our top data and analytics predicts for 2019 [Accessed July 4, 2020, https://blogs.gartner.com/andrew_white/2019/01/03/our-top-data-and-analytics-predicts-for-2019/].

Yayla, A. A., & Hu, Q. (2011). The impact of information security events on the stock value of firms: The effect of contingency factors. *Journal of Information Technology*, *26*(1), 60–77.