Accounting and Management Information Systems
Vol. 21, No. 3, pp. 452-470, 2022
DOI: http://dx.doi.org/10.24818/jamis.2022.03007

Security breaches and modifications on cybersecurity disclosures

Jacob Peng[1, a] and Chang-Wei Li [b]

[a] *Department of Accounting and Taxation, Robert Morris University, USA*
[b] *Department of Accountancy and Graduate Institute of Finance, National Cheng Kung University, Taiwan*

Abstract

Research Question: How do firms approach their cybersecurity disclosure obligations, especially for those who experienced a cyber-attack? Prior research has found that year-after-year modification on textual disclosures adds more appreciable information that makes it more relevant. But do firms provide meaningful disclosures to promote market transparency?

Motivation: Because of growing cybersecurity threats in recent years, the U.S. Securities and Exchange Commission (SEC) has issued several regulations and guidance that emphasized on the disclosure of material information on cybersecurity. Given that the mandatory risk factor disclosures in SEC Form 10-K is the first place firms are encouraged to disclose cybersecurity-related assessment, it is important to examine how firms approach their disclosure expectations.

Idea: To examine whether firms respond to cyber-attacks with meaningful disclosures, we use the Vector Space Model (VSM) to calculate disclosure modifications before and after major cyber-attack incident. **Data**: We extracted cybersecurity breach incidents from the Data Breach Database, a centralized and global database of data breaches maintained by a leading security company. In addition, we use the SEC data depository to find firms' 10-K disclosures.

Findings: We find that firms modify their cybersecurity disclosures by increasing the quantity of disclosures, but not necessarily the quality of disclosures as measured by document similarity. Furthermore, we find partial evidence that the degree of modification is positively associated with the severity of cyber-attacks.

Contribution: Our evidence suggests that firms tend to use boilerplate language to disclose cybersecurity-related issues. This finding is consistent with prior research. That is, consistent

[1] *Corresponding author:* Jacob Peng, Ph.D., CISA, Richard J. Harshman Professor of Accounting, Department of Accounting and Taxation, School of Business, Robert Morris University, USA. Tel. (+1) 412-397-6385, email address: peng@rmu.edu

with prior literature, the information content in public company 10-Ks is limited. We find that this seems to be the case as well when it comes to cybersecurity disclosures.

Keywords: cybersecurity, text analytics, VSM, risk factor

JEL codes: M41

1. Introduction

Cybersecurity has been a growing threat to capital markets and public companies globally. In his speech to staff in the Office of the Director of National Intelligence in July 2021, President Biden warned that the consequence of cyber-attacks is real and dangerous, and such attacks can end up with a "real shooting war with a major power." According to former SEC Chairwoman Mary Jo White, these threats are of extraordinary and long-term seriousness. Cyber threats even surpass terrorism as the most serious threat to the U.S. national interest (SEC, 2014). Cyber incidents can be a result of employee negligence, fraud, organized crime, or even state-sponsored terrorism. The financial and reputational loss due to these attacks can be significant – a recent cyber fraud through fraudulent emails detected in nine companies by the SEC had an estimated loss of nearly $100 million. The FBI estimated that just the cyber fraud through emails along had caused businesses $5 billion since 2013 (SEC, 2018). As a response, the SEC first issued a staff guidance on disclosure obligations relating to cybersecurity risks and cyber incidents in 2011, and then a statement and interpretive guidance on cybersecurity disclosures in 2018 (Peng & Krivacek, 2020).

The 2011 SEC guidance was issued by the SEC's Division of Corporate Finance staff, expressing the guidance on disclosing cyber security-related risks as more and more businesses are experiencing cyber incidences. As cyber-attacks got more and more advanced and severe, the SEC concluded that a more detailed and specific disclosure requirements are needed. Thus, the agency issued the "Statement and Interpretive Guidance on Public Company Cybersecurity Disclosures" in 2018, documenting the required disclosures of cyber risks, incidence, and controls that are needed in public companies' financial reporting function. The goal of these guidance and statements is to timely disclose cyber incidence and its related operation risks and financial impact. Other regulators and stock exchanges also had a number of guidance and requirements on cybersecurity-related disclosures[i]. The attention from regulators and government agencies is the testament that the information asymmetry exists between firms and the general public, and the disclosures requirement is a way to mitigate the gap and promote public interest.

However, with all the disclosure requirements in place, the golden question is, do firms actually make meaningful disclosures on cybersecurity? After all, there's a

potential that disclosing too much information would have an adverse impact on firms. The SEC rules also recognize the importance of finding that balance – disclosing material information that's enough to be relevant to market participants but at the same time, the information related to cybersecurity shouldn't be too details in a way that the "roadmap" is revealed to potential perpetrators (SEC, 2011). The purpose of this research is to examine this balance between public good and company secrecy and confidentiality – what kind of disclosure behaviors do companies exhibit? When companies fall victims of cyber-attacks, do they change what and how they disclose? To study these questions, we adopt text analysis techniques (Janvrin & Fisher, 2021) to review textual discourses made by public companies in the U.S. on the item 1a of the 10-K disclosure. Item 1a is for firms to discuss the risk factors that are significant to their business operations. Both the 2011 guidance and 2018 statement by the SEC suggest firms to consider cybersecurity as a risk factor and determine whether such risk is material that warrants disclosures. These disclosures are required to be specific, that the firms should address how cyber risks apply to them and the firm's response to manage such risk. We measure the disclosure behaviors by calculating the number of words used to describe cybersecurity, the number of cybersecurity-related risk factors disclosed, and how firms modify their cybersecurity disclosures after a known cyber incident. Our results show that firms do change their reporting behavior after a known attack, but these changes may not be completely meaningful – our data shows that firms increased the number of risk factors and the number of words used to describe these risk factors after the attack. However, when we compare the degree of modification on item 1a disclosures on cybersecurity before and after the attack, we fail to find significant differences between the two. As a matter of fact, a number of firms in our sample have identical item 1a disclosures on cybersecurity even after a known cybersecurity incident.

We also control the firm differences to test whether the severity of cyber incidence contributes to the changes in disclosure behavior. Again, we find that firms increased the quantity of disclosures but not the quality, and the severity of attacks is related to the quantity changes but not the quality of cybersecurity disclosures.

This paper is organized as follows. Section 2 provides background of prior research and proposes research hypotheses, followed by the section that explains our methodology and how our variables of interest are defined and measured. Section 4 reports the results of our empirical study and finally, we discuss conclusions and future research in Section 5.

2. Literature review and hypotheses development

Since almost all businesses today operate with heavy dependence on digital technologies, the threat on cybersecurity has grown exponentially. However, for most companies this area is a new frontier that requires a different thinking to face

and manage the risk. For the general public, they usually are not made aware of any breaches until significant damages had been done. This information asymmetry and the need to protect investors led the SEC to issue "CF Disclosure Guidance: Topic No. 2 – Cybersecurity" (the "Guidance") on October 11, 2011. Since the issuance of the 2011 Guidance, the SEC has issued a number of staff comments to companies across different industries demanding more detailed disclosures about their cyber incidents (Gerber & Lowder, 2012). Although technically, the Guidance is not the SEC rulings, failure to address these regulator concerns can still have significant impact. For example, Altaha (formerly known as Yahoo!) was fined $35 Million for failing to disclose one of the largest data breaches in history (SEC, 2018; Peng & Krivacek, 2020).

As companies are becoming more connected than ever to operate, the risk of cybersecurity breaches continues to rise. The 2011 "Guidance" by the SEC was upgraded in 2018 that the SEC adopted "Commission Statement and Guidance on Public Company Cybersecurity Disclosures" (the "Statement") on February 21, 2018. The 2018 Statement not only strengthens the regulator's stand on public companies' obligations under current security laws to disclose cybersecurity risks and incidents, but it also expands the coverage of cybersecurity from the impact on companies' operations to that on other digital assets such as customer information. The "Statement" also emphasizes on the need to create and maintain disclosure controls and means to prevent insider trading during cyber incident.

Both the "Guidance" and the "Statement" suggest companies to disclose cybersecurity risks and incidents in five possible areas in the 10-Ks: risk factors, MD&A, description of business, legal proceedings and financial statement disclosures. However, the item 1a "risk factors" has been the main area where companies choose to disclose cybersecurity risks and incidents and where the SEC focuses on its 10-K reviews (Gerber & Lowder, 2012).

The Guidance demands companies to disclose cybersecurity risks as well as the actual incidents. It is not hard to understand that most companies are reluctant to disclose too much information, especially cyber incidents usually imply significant reputation cost on top of actual lost due to the breach. Although the Guidance is technically not a ruling, the SEC still examines cybersecurity disclosures carefully and issued letters to some companies citing inadequate cybersecurity disclosures (Grant & Grant, 2014).

Accounting researchers had been using modifications to textual disclosures as a measure of disclosure quality. For example, Brown and Tucker (2011) analyzed Management Discussion and Analysis (MD&A) disclosures from company 10-Ks and calculated the year-over-year modification scores. They find that companies generally increase the length of MD&A disclosures, but the modification score tend to decrease over time. This finding suggests that the amount of new information and

information content available to the public from 10-Ks is limited (Li, 2010). Johnson (2018) compared the 10-Ks before and after the issuance of the "Guidance" and found that most companies increased their cybersecurity risk disclosures, but less than half of companies she examined disclosed specific risks and incidents (Johnson, 2018), suggesting companies use boilerplate language to meet their disclosure obligations. This phenomenon is certainly not new, as empirical evidence suggests that firms have already done that in other textual disclosures (Brown & Tucker, 2011). To further examine firms' cybersecurity disclosures, Berkman *et al*. (2018) developed a cybersecurity awareness score based on the 10-K disclosures and found that the market values the amount and relevance of cybersecurity disclosures (Berkman *et al*., 2018).

In summary, we propose the following hypotheses to address our first research questions about the quantity of disclosures after they fall victim of such attacks:

H1a: Firms respond to cybersecurity breaches with increased disclosures measured by the number of cyber-related risk disclosures

H1b: Firms respond to cybersecurity breaches with increased disclosures measured by the number of words in cyber risk disclosures

Empirical studies generally support that the market responds favorably to cybersecurity disclosures (Berkman *et al*., 2018; Gordon *et al*., 2010). Not only these disclosures affect stock prices positively, but they also signal the market that the firm takes their disclosure responsibility seriously. As major industry organizations like AICPA suggests, cybersecurity should be part of the corporate risk management program that considers risks and benefits simultaneously and subject to periodic assessment (American Institute of Certified Public Accountants (AICPA), 2018). In a research synthesis conducted by Haapamaki & Sihvonen (2019), disclosures and cybersecurity activities are one of the most-researched, but also the research stream that need more attention given how interconnected businesses are today (Haapamaki & Sihvonen, 2019). As previously mentioned, the SEC guidance and statement both emphasize the importance to strive for the balance of firm confidentiality and public good. However, the voluntary nature of qualitative disclosures like disclosing cyberattacks is still subject to heavy management discretion. Hausken (2007) presented a classic dilemma of a free-rider problem when it comes to diclosing cybersecuiry matters (Hausken, 2007). From the market perspective, disclosing cyberattacks promotes market transparency. For companies in the same industry, if someone discloses a recent cyberattack it definitely helps the other company prevent the similar attack or uses the opportunity to patch the security programs to mitigate the risk. However, this ideal situation usually doesn't happen as firms will want to exploit others' security expenditures (Haapamaki & Sihvonen, 2019) and have a perfect incentive to be a free-rider without any external intervention (Gordon *et al*.,

2015). As a result, regulations such as the SEC guidance and statement play a critically important role in promoting public good and market transparency.

However, regulations do not necessarily address the practical implications of optimal disclosures – whether firms actively engage in meaningful disclosures is still a questionable assumption. For example, the literature already document that firms withhold sensitive and discretionary information items (Amir & Ziv, 1997; Kasznik & Lev, 1995). Amir *et al*. (2018) documented that managers do not disclose negative information related to cyber-attacks because they think the information will remain private and investors are not able to independently discover or verify (Amir *et al*., 2018). Other than the reputation effect and compliance requirements, research has suggested that firms disclose cybersecurity matters can actually benefit themselves. For example, Wang *et al*. (2013) found that disclosing actionable information that mitigates risk is associated with less severe future security incidents (Wang *et al*., 2013). In other words, the practice of disclosing better-quality security information would reward the companies with fewer future security breaches. This might explain that why firms voluntarily disclose security matters in the SOX report even when the regulation doesn't require it (Haapamaki & Sihvonen, 2019). Gordon *et al*. (2006) documented that firms disclosing significantly more security-related matters after SOX (2002) passed – when the law didn't require such disclosures (Gordon & Loeb, 2006). In addition to *what* the firms disclose about security issues, *when* the firm make such disclosures also matter. Amir *et al*. (2018) documented a 118% improvement in security price decline if the firm discloses cyber-attacks within three days, compared to the one who waits for a month (Amir *et al*., 2018). As such, it is not a surprise that managers choose to withhold information related to breaches and security matters for various reasons (Baginski *et al*., 2018; Southwell *et al*., 2017).

The debate of whether cybersecurity disclosures works is ongoing and the literature is inconclusive regarding the market reaction to cybersecurity disclosures (Campbell *et al*., 2003; Cavusoglu *et al*., 2004; Gordon *et al*., 2011; Kannan *et al*., 2007). Intuitively, one would think such disclosures will work as mentioned earlier to solve the free-rider problem. However, Li *et al*. (2018) found that cybersecurity disclosures are not necessarily associated with future security breaches, indicating that the value of such disclosures may be limited (Li *et al*., 2018). As a result, it is important to further study how the firms respond to their disclosure obligations (Haapamaki & Sihvonen, 2019) as more and more regulations regarding the disclosure requirements are in place or being proposed (Freund, 2022; SEC, 2022). We propose to study the pre- and post-attack disclosure differences both in terms of the quantity and quality of cybersecurity disclosures in order to help us better understand the impact on cybersecurity risk management:

H2: The severity of cybersecurity breaches has positive impact on the *quantity* of firms' cybersecurity disclosures

H3: The severity of cybersecurity breaches has positive impact on the *quality* of firms' cybersecurity disclosures

3. Methodology and data

This research tests whether firms respond to cybersecurity breaches by meaningfully disclosing the cybersecurity incidents. Prior research had found that the companies do not always disclose clear and unbiased textual information as this form of corporate disclosures is subject to management manipulation (Li, 2010). When it comes to cybersecurity disclosures, companies have a lot of discretions as to determine whether any incident is material enough to warrant disclosing the details. To examine this potential change in disclosure behavior, we investigate changes in cybersecurity disclosures, particularly the changes in quantity and quality of cybersecurity disclosures before and after the cybersecurity breaches.

We extracted cybersecurity breach incidents from the Data Breach Database[ii], a centralized and global database of data breaches maintained by a leading security company. In addition to track publicly available breaches in different industries and breach types, this database also calculates the severity of breaches (called Breach Level Index, BLI) by using factors such as the number of records affected, the type of data breached, the source of breach, and how information was used. We started with all breaches captured by the database in 2013 – 2016. We removed all breaches related to non-public companies and resulted to 38 incidents with valid disclosure data[iii].

Since the main source of cybersecurity breach disclosure is in the item 1a "Risk Factors" of the Form 10-K filed by public companies, we focused our effort on identifying cybersecurity risks and cyber incidents disclosed in this section of the Form 10-K. We extracted the 10-Ks before and after the cyber incidents from the SEC website for firms with reported breaches. For each incident, we extracted and located two disclosures: $[\text{StockTicker}]_{\text{pre}}$ and $[\text{StockTicker}]_{\text{post}}$. To prepare these textual disclosures for analysis, we clean up these disclosures by following these steps:

1. Remove editorial words (section titles, page number, table of contents, etc.)
2. Remove disclaimers and cautionary language such as "*Information required by this Item is included in the Annual Report under the heading "Risk Factors" on pages X through Y which is incorporated herein by reference pursuant to General Instruction*."
3. We also extracted item 1a paragraphs that contained the following keywords: cyber, attack, malicious, security[iv], and breach.

The variables of interest to test our hypotheses are the quantity and quality of disclosures before and after the recorded breaches. We used the number of risk factors (RF, each RF is a paragraph that contains our keywords) and the number of words[v] in each RF as the measures of the disclosure quantity:

changes in the number of risk factors in cybersecurity disclosures

$$\Delta RF = RF_{post} - RF_{pre}$$

changes in the number of words in cybersecurity disclosures

$$\Delta WORD = WORD_{post} - WORD_{pre}$$

The quality of disclosures is measured by how similar (SIMILARITY) it is for firms to disclose cybersecurity risks and breaches after the incidents. If such disclosure after the incident is very similar to that before the incident, we can reasonably argue that the quality of such disclosure is low. That is, we expect the cybersecurity disclosure to be different significantly after the cyber incidents. We use the cosine similarity method to construct our RF disclosure quality score.

The cosine similarity is based on vector space model (VSM) initially proposed by Salton and McGill (Salton & McGill, 1983). This model has traditionally used by search engines to calculate document similarities to yield results such as "Find Similar Documents" (Brown & Tucker, 2011). The VSM compared term vectors found in document A and B, and the smaller angle represents more similar documents, where θ represents the angle between vector A and vector B. Each vector is comprised of all terms found in the document:

$$\text{similarity} = \cos(\theta) = \frac{A \cdot B}{\|A\|\|B\|} = \frac{\sum_{i=1}^{n} A_i \times B_i}{\sqrt{\sum_{i=1}^{n} (A_i)^2} \times \sqrt{\sum_{i=1}^{n} (B_i)^2}}$$

The score is bounded between 0 and 1 with cos(θ) = 0 represents identical documents. Figure 1 provides a visual representation of how similarity (θ) is determined by calculating the angle between pre- and post- disclosures.

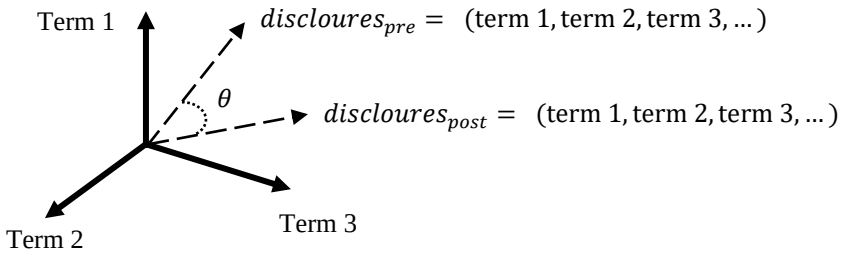
We follow Brown and Tucker (2011) to calculate document vectors, using TF-IDF weighting function. TF-IDF is "term frequency" (TF) multiplied by "inverse document frequency" (IDF). TF is "The weight of a term that occurs in a document", and IDF is "if it's common or rare across all documents". We focus on pre-post difference (two documents) of cybersecurity disclosures, so we do not use IDF. The following is the formula of TF.

$$TF_{ij} = term_i / doucment_j$$

$term_i$: the number of times that term i occurs in document j

$doucment_j$: the number of all term in document j

Figure 1. Visual Representation of the VSM Similarity Calculation between Pre- and Post-Disclosures



In addition, we adopt the following analytical procedures to calculate θ:

1. Delete punctuation marks, stemming, delete stop words, and case normalization (Miner *et al*., 2012).
2. Calculate document vector by term frequency (TF).
3. Calculate cosine similarity by document vector.

The list of firms and breaches included in our sample are reported in Table 1.

Since cyber breaches are common landscape among modern businesses, they are not merely yes or no issue – rather, the breach severity and ramifications are wildly different (Stiennon, 2013). As a result, we are also interested in examining whether the breach severity contributes to firms' different reactions when it comes to disclosing cyber security risks and incidents. We use the following model to test the relationship between breach severity and disclosures:

$$[\text{Disclosure}] = \beta_0 + \beta_1 [\text{Breach severity}] + \beta_2 [\text{Control variables}] + \varepsilon$$

As previously described, we use the changes in the number of risk factors in cybersecurity disclosures (ΔRF) and the changes in the number of words in cybersecurity disclosures ($\Delta WORD$) as the measure of disclosure quantity. The quality of disclosure is measured by the cosine similarity between the firm's PRE and POST item 1a disclosures. The breach severity is measured by the number of records breached and the Breach Level Index (BLI) calculated by the Data Breach Database. We control the firm differences by incorporating the reported sales revenue in the breach year.

4. Results

To examine our first research question: did firms respond to cybersecurity breaches by updating their cyber disclosures? We first test the quantitative difference of disclosures before and after the incident. We compare item 1a on the 10-K published immediately before and after the cyber incident. The variables used to test the quantitative difference *post* the cyber incident are the number of risk factors disclosed, the number of words used in risk factor disclosures, and the total number of words in item 1a disclosure.

Table 1. List of breaches included in analysis

Firm Name (Ticker)	Industry	Date Breached	Records Breached	Breach Source
American Airlines (AAL)	Other	1/13/2015	10,000	Malicious Outsider
Apple/ Iphone (AAPL)	Retail	9/1/2015	225,000	Malicious Outsider
AECOM (ACM)	Technology	6/2/2014	52,660	Malicious Outsider
Adobe Systems (ADBE)	Technology	9/18/2013	152,000,000	Malicious Outsider
AOL (AOL)	Technology	4/28/2014	2,000,000	Malicious Outsider
American Express (AXP)	Financial	3/25/2014	76,608	Malicious Outsider
AutoZone (AZO)	Retail	8/9/2015	50,000	Malicious Outsider
Citigroup (C)	Financial	6/27/2013	150,000	Malicious Outsider
Coca-Cola (CCE)	Retail	1/24/2014	74,000	Malicious Outsider
Comcast (CCV)	Other	4/30/2015	1,200	Malicious Insider
Costco (COST)	Retail	7/15/2015	2,200	Malicious Outsider
Salesforce (CRM)	Technology	9/3/2014	2,000,000	Malicious Outsider
eBay (EBAY)	Retail	5/21/2014	145,000,000	Malicious Outsider
Express Scipts (ESRX)	Financial	2/13/2013	20,000	Malicious Outsider
Entercom (ETM)	Other	2/28/2014	13,000	Malicious Outsider
Facebook (FB)	Technology	6/2/2013	6,000,000	Accidental Loss
Hanesbrands (HBI)	Retail	6/9/2015	900,000	Malicious Outsider
Home Depot (HD)	Retail	9/2/2014	109,000,000	Malicious Outsider
IberiaBank Corp (IBKC)	Financial	5/6/2014	12,000	Malicious Insider
JPMorgan Chase (JPM)	Financial	8/27/2014	83,000,000	Malicious Outsider
Lowe's (LOW)	Retail	4/2/2014	35,000	Accidental Loss
Monsanto Company (MON)	Other	3/27/2014	1,600	Malicious Outsider
Morgan, Chase (MS)	Financial	7/14/2014	15,000	Malicious Outsider
Netflix (NFLX)	Other	10/30/2015	2,000	Malicious Outsider

Firm Name (Ticker)	Industry	Date Breached	Records Breached	Breach Source
Quad/Graphics (QUAD)	Retail	8/19/2015	693	Malicious Outsider
Rite Aid (RAD)	Retail	2/3/2016	976	Malicious Outsider
Staples (SPLS)	Retail	10/21/2014	1,160,000	Malicious Outsider
AT&T (T)	Retail	8/8/2014	1,600	Malicious Insider
Target (TGT)	Retail	11/4/2013	110,000,000	Malicious Outsider
The Timken Company (TKR)	Other	1/30/2014	4,983	Malicious Outsider
UPS (UPS)	Retail	8/11/2014	105,000	Malicious Outsider
Walgreen (WBA)	Retail	8/7/2015	8,345	Malicious Outsider
Wells Fargo (WFC)	Financial	8/13/2013	1,800	Malicious Outsider
Time Warner Cable (TWX)	Other	1/8/2016	320,000	Malicious Outsider
Sprouts (SFM)	Retail	3/16/2016	21,000	Malicious Outsider
Carbonite (CARB)	Technology	6/21/2016	1,500,000	Malicious Outsider
Apple Inc (AAPL)	Technology	3/7/2016	6,500	Malicious Outsider
Kroger (KR)	Retail	5/4/2016	431,000	Malicious Outsider

As Table 2, Panel A indicates, firms who suffered cyber-attacks did increase the amount of disclosures, as measured by the number of relevant risk factors disclosed and the number of words used to describe these risk factors. Firms increased 0.763 risk factor paragraphs and used on average 89.58 more words to describe cybersecurity-related disclosures, which represent 37.56% increase in number of risk factors discussed and 35.7% increase in the number of words used to describe these risk factors. Panel 2b reports the results of test of mean differences. Both differences are significant (p=0.002 and 0.006, respectively). To better illustrate the changes in disclosures after a cyber incident, Appendix A shows a 10-K item 1a disclosure from Sprouts Farmers Market Inc (NASDAQ: SFM), who was a victim of a cyber breach in March 2016. The company discussed a new incident in its fiscal year 2016 10-K, by describing the nature of the breach as well as remediation initiatives. The quantity of cybersecurity-related disclosures increased by 79% for this company. Interestingly, the difference in total number of words used in item 1a disclosure on 10-Ks is not significantly different *post* the cyber incidents, indicating that firms shifted their emphasis in item 1a from other areas to cybersecurity-related risk factors disclosures. H1a and H1b are supported.

Table 2. Empirical results

Panel 2a. Descriptive statistics

	Mean		Max.		Min.	
Variable	**PRE**	**POST**	**PRE**	**POST**	**PRE**	**POST**
Number of cyber risk disclosures (RF)	2.05	2.82	6.00	7.00	0	0
Number of words in cyber risk disclosures (WORD)	250.89	340.47	598.00	1,049.00	38.00	38.00
Number of total words in item 1a.	7,973.61	9,786.79	37,841.00	82,414.00	620.00	827.00
Cosine similarity score (SIMILARITY)	0.85		1.00		0.36	
Percentage (%) increase POST-PRE						
Number of cyber risk disclosures (RF)	37.56%		16.67%		0	
Number of words in cyber risk disclosures (WORD)	35.70%		75.42%		0	
Number of total words in item 1a.	22.74%		117.79%		33.39%	

Panel 2b. Test of mean difference (POST-PRE)

	Mean				
Variable	**PRE**	**POST**	**Mean Difference (POST-PRE)**	**t**	**Significance**
Number of cyber risk disclosures (RF)	2.05	2.82	0.763	3.307	0.002**
Number of words in cyber risk disclosures (WORD)	250.89	340.47	89.579	2.947	0.006**
Number of total words in item 1a.	7,973.61	9,786.79	1,813.184	0.982	0.333

Table 3. Test of severity and firm response

Model 1: [Disclosure quantity/quality] = β_0 + β_1 [Records breached] + β_2 [Revenue] + ε

(Dependent variable = ΔRF ; adjusted R^2=0.412)

Independent Variable	Sign	*p*
Constant	+	0.297

Model 1: [Disclosure quantity/quality] = β_0 + β_1 [Records breached] + β_2 [Revenue] + ε

# of records breached	+	0.000 **
Revenue	+	0.403

(Dependent variable = $\Delta\ RF$; adjusted R^2=0.324)

Independent Variable	Sign	*p*
Constant	+	0.429
# of records breached	+	0.000 **
Revenue	+	0.422

(Dependent variable = SIMILARITY; adjusted R^2=-0.033)

Independent Variable	Sign	*p*
Constant	+	0.000
# of records breached	-	0.396
Revenue	-	0.764

Model 2: [Disclosure quantity/quality] = β_0 + β_1 [BLI score] + β_2 [Revenue] + ε

(Dependent variable = $\Delta\ RF$; adjusted R^2=0.409)

Independent Variable	Sign	*p*
Constant	-	0.000
BLI score	+	0.000 **
Revenue	+	0.329

(Dependent variable = $\Delta\ WORD$; adjusted R^2=0.381)

Independent Variable	Sign	*p*
Constant	-	0.000
BLI score	+	0.000 **
Revenue	+	0.323

(Dependent variable = SIMILARITY; adjusted R^2=-0.037)

Independent Variable	Sign	*p*
Constant	+	0.000
BLI score	-	0.443

Model 1: [Disclosure quantity/quality] = β_0 + β_1 [Records breached] + β_2 [Revenue] + ε			
Revenue	ΔRF	-	0.751

Next, we turn to our test of whether the severity of cyber incidents had anything to do with the firms' disclosure behavior. That is, do firms respond more meaningfully when they are the victims of more severe attacks? The regression test results are reported on Table 3. As the results indicate, firms responded with more disclosures to more severe cyber incidents, measured by both the number of records breached and the BLI score, H2 is supported. In terms of the quality of disclosures, the mean document similarity score measured by cosine similarity using the VSM model is 0.85. Unfortunately, our data does not support that companies' alterations of their cybersecurity disclosures are affected by how severe they were breached. H3 is not supported.

5. Conclusions

This paper examines how firms respond to cybersecurity attack by disclosing their related risk factors. Cybersecurity disclosure is a hot topic that the academics and practitioners have debated how the balance between public interest and firm confidentiality should be addressed. We believe this research is an important first step to understand both quantity and quality of cybersecurity disclosures when firms suffer cyber-attacks.

Using security breaches data in the U.S., we find that companies do adjust their cybersecurity-related disclosures. Companies respond to cyber-attacks by increasing the amount of disclosures: companies disclose 35.7% more when they are cyber-attack victims. However, our evidence does not find the quality of disclosures as measured by document similarities changes due to cyber-attacks. The fact that post-attack disclosures are still similar to the pre-attack ones confirms the SEC's argument that firms use boilerplate disclosures and thus more guidance and regulations are necessary to advocate for more meaningful cybersecurity disclosures.

Our evidence suggests that firms tend to use boilerplate language to disclose cybersecurity-related issues. This finding is consistent with prior research (Brown & Tucker, 2011; Li, 2010; Johnson, 2018). That is, consistent with prior literature, the information content in public company 10-Ks is limited. We find that this seems to be the case as well when it comes to cybersecurity disclosures.

Prior literature also suggests that managers exercise a lot of discretion to determine what companies voluntarily disclose (Wang *et al*., 2013; Gordon & Loeb, 2006; Amir & Ziv, 1997). Our results show that firms do not always disclose meaningful

cybersecurity-related information, as evidenced by an insignificant difference in document similarity score comparing pre- and post-security breaches. Our results do suggest that companies increase the amount of disclosures after a known cyber-incident by shifting more focus from other risk factors discussions to cybersecurity-related content in firms' 10-K item 1a disclosures.

Future research may be extended to examine other measures of disclosure quality, as more and more companies fell victims of cyber-attacks. The technology advancements and more sophisticated cybercriminals have made the cybersecurity landscape more complicated than ever. Public companies across the globe have the obligation to disclose material information to their stakeholders. However, keeping the balance between their disclosure obligation and protecting shareholder interest cannot be achieved if we do not understand how companies respond to this kind of requirements. Regulators also need to understand the impact of regulations in order to be a good steward of public interest in capital markets. In addition, studying disclosure behavior becomes more and more important when the E.U., the U.S., and other jurisdictions around the world develop and implement more cybersecurity disclosure mandates and regulations.

References

American Institute of Certified Public Accountants (AICPA) (2018) "Cybersecurity risk management reporting fact sheet", available on-line at: https://us.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/cybersecurity/ [Accessed 1 February 2022]

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

Amir, E. & Ziv, A. (1997) "Recognize, disclose, or delay: Timing the adoption of SFAS No. 106", *Journal of Accounting Research*, vol. 35(Spring): 61-81

Baginski, S. P., Campbell, J. L., Hinson, L. A. & Koo, D. S. (2018) "Do careers concerns affect the delay of bad news disclosure?", *The Accounting Review*, vol. 93, no. 2: 61-95

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

Brown, S. V. & Tucker, J. W. (2011) "Large-sample evidence on firms' year-over-year MD&A modifications", *Journal of Accounting Research*, vol. 49, no. 2: 309-346

Campbell, K., Gordon, L., Loeb, M. & Zhou, L. (2003) "The economic cost of publicly announced information security breaches: Empirical evidence from the stock market", *Journal of Computer Security*, vol 11: 431-448

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*, vol. 9: 69-104

Freund, J. (2022) "The future of quantitative cyberrisk reporting, available on-line at: https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2022/volume-23/the-future-of-quantitative-cyberrisk-reporting. [Accessed 9 June 2022]

Gerber, A. & Lowder, J. (2012) "Cybersecurity disclosure: SEC's Expanding disclosure initiatives & expectations", *The Corporate Governance Advisor*, vol. 20, no. 6: 11-21

Gordon, A. L. & Loeb, P. M. (2006) *Managing Cybersecurity Resources*. New York: McGraw Hill

Gordon, L., Loeb, M., Lucyshyn, W. & Zhou, L. (2015) "The impact of information sharing on cybersecuirty underinvestment: A real options perspective" *Journal of Accounting and Public Policy*, vol. 34, no. 5: 209-519

Gordon, L., Loeb, M. & Sohail, T. (2010) "Market value of voluntary disclosures concerning information security", *MIS Quarterly*, vol. 34, no. 3: 567-594

Gordon, L., Loeb, M. & Zhou, L. (2011) "The impact of information security breaches: Has there been a downward shift in costs?", *Journal of Computer Security*, vol. 19: 33-56

Grant, G. H. & Grant, C. T. (2014) "SEC cybersecurity disclosure guidance is quickly becoming a requirement", *The CPA Journal*, vol. 2014(May): 69-71

Haapamaki, E. & Sihvonen, J. (2019) "Cybersecurity in accounting research", *Managerial Auditing Journal*, vol. 34, no. 7: 808-834

Hausken, K. (2007) "Information sharing among firms and cyber attacks", *Journal of Accounting and Public Policy*, vol. 26, no. 6: 639-688

Janvrin, D. & Fisher, I. (2021) "Textual analysis for accountants", *Strategic Finance*, Vol. 2021(June): 46-53

Johnson, G. F. (2018) "Examining cybersecurity risk reporting on US SEC form 10-K", *ISACA Journal*, vol. 4: 1-8

Kannan, A., Rees, J. & Shridhar, S. (2007) "Market reactions to information security breach announcements: An Empirical analysis", *International Journal of Electronic Commerce*, vol. 12: 69-91

Kasznik, R. & Lev, B. (1995) "To warn or not to warn: Management disclosures in the face of an earnings surprise", *The Accounting Review*, vol. 70, no. 1: 113-134

Li, F. (2010) "Textual analysis of corporate disclosures: A Survey of the literature", *Journal of Accounting Literature*, vol. 29: 143-165

Li, F. (2010) "The information content of forward-looking statements in corporate filings - A naive Bayesian machine learning approach", *Journal of Accounting Research*, vol. 48, no. 5: 1049 - 1102

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

Miner, J., Delen, D., Elder, J., Fast, A., Hill, T. & Nisbet, R. (2012) *Practical Text Mining and Statistical Analysis for Non-Structured Text Data Applications*, Amsterdam:Elsevier Science & Technology

Peng, J. & Krivacek, G. (2020) "The growing role of cybersecurity disclosures", *ISACA Journal*, vol. 2020 (January): 1-7

Salton, G. & McGill, M. (1983) *Introduction to modern information retrieval*, New York: McGraw-Hill

SEC (2011) "CF disclosure guidance: Topic no. 2", available on-line at: https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm [Accessed 1 February 2022]

SEC (2014) "Opening statement by SEC Chair Mary Jo White", available on-line at: http://www.sec.gov/News/PublicStmt/Detail/PublicStmt/1370541286468 [Accessed 1 February 2022]

SEC (2018) "Altaba, formerly known as Yahoo!, charged with failing to disclose massive cybersecurity breach; agrees to pay $35 million", available on-line at: https://www.sec.gov/news/press-release/2018-71 [Accessed 1 February 2022]

SEC (2018) "SEC investigative report: Public companies should consider cyber threats when implementing internal accounting controls", available on-line at: https://www.sec.gov/news/press-release/2018-236 [Accessed 1 February 2022]

SEC (2022) "SEC proposes rules on cybersecurity risk management, strategy, governance, and incident disclosure by public companies", available on-line at: https://www.sec.gov/news/press-release/2022-39 [Accessed 9 June 2022].

Southwell, A., Vandevelde, E., Bergsieker, R. & Bisnar-Maute, J. (2017) "Gibson Dunn reviews U.S. cybersecurity and data privacy", available on-line at: https://clsbluesky.law.columbia.edu/ [Accessed February 2022]

Stiennon, R. (2013) *Categorizing data breach severity with a Breach Level Index*, Belcamp, MD: SafeNet, Inc.

Wang, Y., Kannan, K. & Ulmer, J. (2013) "The association between the disclosure and the realization of information security risk factors", *Information Systems Research*, vol. (24), no. 2: 201-218

Appendix A: Sample Item 1a. Disclosures Before and After a Known Cyber-incident

Sprouts Farmers Market Inc (NASDAQ: SFM)
Breach Date = 3/16/2016

SFM's Item 1a in its 10-K dated December 31, 2015 (BEFORE the breach)
Disruptions to, or security breaches involving, our information technology systems could harm our ability to run our business. We rely extensively on information technology systems for point of sale processing in our stores, supply chain, financial reporting, human resources and various other processes and transactions. Our information technology systems are subject to damage or interruption from power outages, computer and telecommunications failures, computer viruses, security breaches, including breaches of our transaction processing or other systems that could result in the compromise of confidential customer data, catastrophic events, and usage errors by our team members. In January 2013, we discovered sophisticated malware installed on certain credit card "pin pads" in a limited number of our stores designed to illegally access our customers' credit card information. We discovered the malware shortly after it was planted and promptly shut down its access to our systems. In connection with the January 2013 breach, in addition to replacing the affected card terminals for a total cost of approximately $170,000, we engaged a nationally recognized cybersecurity firm to investigate the incident. The costs associated with the investigation, and penalties assessed by our credit card vendors, are covered by our insurance policy, subject to our insurance deductible of $100,000. We have implemented numerous additional security protocols since the attack in order to further tighten security, but there can be no assurance similar breaches will not occur in the future, be detected in a timely manner or be covered by our insurance policy.
SFM's Item 1a in its 10-K dated December 31, 2016 (AFTER the breach)
Disruptions to, or security breaches involving, our information technology systems could harm our ability to run our business. We rely extensively on information technology systems for point of sale processing in our stores, supply chain, financial reporting, human resources and various other processes and transactions. Our information technology systems are subject to damage or interruption from power outages, computer and telecommunications failures, computer viruses, security breaches, including breaches of our transaction processing or other systems that could result in the compromise of confidential customer data, catastrophic events, and usage errors by our team members. In March 2016, an email "phishing" scam was perpetrated

against one of our team members, who inadvertently disclosed 2015 W-2 statements of our team members to an unauthorized third party purporting to be one of our executive officers. We worked with the FBI and the IRS to investigate this crime and to determine the best ways to protect team member tax information, and offered credit monitoring services to impacted team members. As described under "Legal Proceedings," we are subject to four complaints related to this scam, each on behalf of a purported class of our current and former team members whose personally identifiable information was inadvertently disclosed; these matters are covered by our cyber insurance, subject to applicable deductibles. Additionally, in January 2013, we discovered sophisticated malware installed on certain credit card "pin pads" in a limited number of our stores designed to illegally access our customers' credit card information. We have implemented numerous additional security protocols since these attacks in order to further tighten security and continue to maintain a customary cyber insurance policy, but there can be no assurance similar breaches will not occur in the future, be detected in a timely manner or be covered by our insurance policy.

Our information technology systems may also fail to perform as we anticipate, and we may encounter difficulties in adapting these systems to changing technologies or expanding them to meet the future needs and growth of our business. If our systems are breached, damaged or cease to function properly, we may have to make significant investments to fix or replace them, suffer interruptions in our operations, incur liability to our customers and others, face costly litigation, and our reputation with our customers may be harmed. Various third parties, such as our suppliers and payment processors, also rely heavily on information technology systems, and any failure of these systems could also cause loss of sales, transactional or other data and significant interruptions to our business. Any material interruption in the information technology systems we rely on may have a material adverse effect on our operating results and financial condition.

[i] Both NYSE and NASDAQ in their listing rules require listed companies to promptly release materials information related to cyber incidences. In addition, U.S. Commodity Futures Trading Commission, Financial Stability Oversight Council, and Financial Industry Regulatory Authority all have similar guidance on cybersecurity issues.

[ii] https://breachlevelindex.com/data-breach-database

[iii] Invalid: first year going public (so no t-1 disclosure), data not available, etc.

[iv] We excluded paragraphs like terrorist attack; or word that was mentioned as a single instance in other paragraphs; such as "…our reputation; inflation, natural disasters, and acts of war or terrorism; the actions and initiatives of current and potential competitors, as well as governments, regulators and self-regulatory organizations; the effectiveness of our risk management policies; and technological changes and risks, including cybersecurity risks; or a combination of these or other factors." We also excluded physical breach or personnel security mentioned in these paragraphs.

[v] We remove stop words from our disclosure samples as many text analytics papers do.