Journal of Cybersecurity Education, Research and Practice

Volume 2019 | Number 2 Article 3

2019

Investigating the impact of publicly announced information security breaches on corporate risk factor disclosure tendencies

Sandra J. Cereola
James Madison University, cereolsj@jmu.edu

Joanna Dynowska
University of Warmia and Mazury in Olsztyn, joannan@uwm.edu.pl

Investigating the impact of publicly announced information security breaches on corporate risk factor disclosure tendencies

Abstract

As the reported number of data breaches increase and senators push for more disclosure regulation, the SEC *staff* issued a guidance in 2011 on disclosure obligations relating to cybersecurity risks and incidents. More recently, on February 26, 2018 the SEC *Commission* issued interpretive guidance to help assist public companies prepare disclosures regarding cybersecurity risks and incidents. As reported incidents of cybersecurity breaches occur, investors are concerned about the risks associated with these incidents and the impact they may have on financial performance. Although the SEC staff guidance warns public companies to make timely disclosure, recognizing the threat that cybercrime poses to investors in the public markets, it does not go far enough to institute direct measures that would compel companies to reveal the nature and scope of a cybersecurity breach.

In light of the lack of specific guidance on cybersecurity disclosure, the aim of this study is to develop a better understanding of the cybersecurity disclosure landscape. The purpose of this study is phenomenological in nature, designed to assess the impact of the 2011 SEC staff guidance on the disclosure of cybersecurity risk factors and provide recommendations for future research following the 2018 SEC Commission's interpretive guidance. This study analyzes the impact of the SEC guidance by investigating risk factor disclosures both before and after the SEC's 2011 issuance date. We pay particular attention to organizations that have suffered a data breach, as determined by the Privacy Rights Clearinghouse (PRC). The study uses companies listed on the S&P 500.

Results show that there has been a 23 percent increase in the number of firms referencing cybersecurity in the Risk Factor section of the 10-K and that factors such as the size of the firm, prior reported breaches and breach type were predictors of disclosure. The study also found that there is a tendency not to disclose reported breaches in the narrative of the 10-K and that the cybersecurity risk factor disclosures do not include details on actual breaches. The underreporting of cyber incidents may be in part be the result of alternative interpretations of what constitutes a "material" breach. This study should be of interest to the SEC, in particular, as they continue to evaluate cybersecurity guidance in terms of its implementation by corporate filers and as they move toward a cybersecurity disclosure *regulation.* In addition, as the SEC continues to scrutinize cybersecurity incident disclosures and issue comment letters to public companies with inadequate disclosures, it should be of interest to corporate filers, as well as to investors, analysts and other professionals that are concerned with the informativeness of corporate cybersecurity disclosures particularly as they affect profits.

Keywords

cybersecurity, data security breach, SEC disclosure

INTRODUCTION

As cybersecurity threats and incidents become more widespread, investors, the Securities and Exchange Commission's (SEC) and other stakeholders are increasingly concerned with how this information is disclosed in public company filings. In a letter signed by five Senators in 2011, the senators suggested that, "inconsistencies in reporting, investor confusion, and the national importance of addressing cyberspace security" demand that the SEC "issue guidance regarding the disclosure of information security risk, including material network breaches" (Rockefeller et al. 2011). Just five months after the letter's release, the SEC staff issued its first guidance on the topic of cybersecurity.

The SEC staff guidance, issued on October 13, 2011, requires all public companies to disclose cybersecurity events if they *materially* affect the company's products, services, relationships or competitive condition. The guidance indicates, "Material information regarding cybersecurity risks and cyber incidents is required to be disclosed when necessary in order to make other required disclosures, in light of the circumstances under which they are made, not misleading" (SEC 2011). More recently, on February 26, 2018, the SEC Commission issued interpretive guidance to assist public companies preparing disclosures regarding cybersecurity risks and incidents, "in light of the increasing significance of cybersecurity incidents" (SEC 2018). This guidance reinforces and expands upon the 2011 SEC staff guidance.

The importance of such guidance is of particular interest to investors in publicly traded companies as reports of cybersecurity incidents are occurring with more frequency in high profile public companies. According to the Identity Theft Resource Center (ITRC) there were 1,579 reported data breaches in 2017 alone (ITRC 2017). This list includes large publicly traded companies such as Equifax, Yahoo, Verizon, Intercontinental Hotels Group, Arby's, VeriFone, and other highly identifiable named companies.

For public companies, the 2011 SEC staff guidance requires disclosure of material adverse cyber incidents. Studies suggest that companies underreport these events due to differing interpretations of the meaning of *materiality* (Young 2013). The 2011 guidance intent was to increase disclosures on cybersecurity risk for public companies. Concerns voiced by senators suggest that the 2011 disclosure guidance is insufficient for investors (Rockefeller 2013), that it is too general and that it does not provide clear instructions on what constitutes a material breach. Without clear guidelines, executives exercise judgment when determing materialtiy, resulting in discrepancies in interpretation and the underreporting of cybersecurity events. Thus, our first research question investigates whether cybersecurity risk factor disclosures increased in light of the

SEC 2011 staff guidance particularly for those companies that have suffered a cybersecurity breach.

Although to date, the SEC has only brought one regulatory enforcement action against a company for failure to disclose a massive cybersecurity breach (SEC Altaba 2018), the SEC has been active in this area by issuing comment letters asking public companies to amend their corporate filings. Beginning in 2012, the SEC issued comment letters to approximately 50 public companies concerning cybersecurity compliance (White 2013). Pressure from the SEC has prompted at least two of these companies to disclose information on known security breaches in their SEC filings (i.e., Amazon and Google) (Sandler 2012), and others were told to improve their disclosure on cyber-risks (i.e., American International Group, Inc., Eastman Chemical Co. and Quest Diagnostics Inc.). In addition to the SEC, the Federal Trade Commission (FTC) has enforced its authority using Section 5 of the FTC Act that prohibits "unfair or deceptive trade practices" FTC (2016) by pursuing companies for alleged cyber security incidents (i.e., LifeLock, ChoicePoint, Twitter, Wyndham Hotels, Dish Network, TJX Companies, etc.) (Giorgianni 2017).

The consequences of these cybersecurity incidents has affected many stakeholders resulting in investors filing class action lawsuits against some of these companies (e.g. Equifax - over 50 class action lawsuits have been filed (Giorgianni 2017); CareFirst, Inc. – class action suit filed in 2015 (Sherman 2015)). Most recently, Yahoo agreed to pay $80 million to settle a class action lawsuit that alleged that Yahoo failed to disclose four data breaches affecting over 3 billion customers (Muncaster 2018) and Anthem agreed to pay $115 million to settle lawsuits from its 2015 data breach (Chew, Newby, Fenwick &West 2017).

Based on the increase in SEC comment letters regarding cybersecurity risk factors, the increase in class action lawsuits against companies with cyber incidents, and the requirement that registrants report cyber incidents if material (including prior incidents), the second research question investigates whether companies that have had past cybersecurity breaches are more likely to include a cybersecurity risk factor in their annual report post 2011 SEC staff guidance.

With the pervasiveness of technology, material cyber incidents pose a threat to all companies regardless of industry. Some industries may be at a higher risk than others; particularly if they gather personally identifiable information. Beyond the SEC requirements, some industries have other regulatory bodies requiring disclosure for certain types of breaches (e.g. Health Insurance Portability and Accountability Act (HIPAA) for healthcare companies, Payment Card Industry Data Security Standard (PCI-DSS) for retailers, etc.). Thus, our third and fourth research question investigates whether type of breach or industry has an impact on cybersecurity risk factor disclosure.

Existing SEC laws require registrants to list in their financial statements a variety of risk factors that could have a material impact on their businesses. Although no existing SEC disclosure ***requirement*****s** specifically refer to cybersecurity, disclosure requirements, as written, "may impose an obligation on registrants to disclose such risks and incidents" (SEC 2011). The purpose of this phenomenological study is to evaluate cybersecurity disclosure tendencies in light of the 2011 SEC staff guidance on cybersecurity risk disclosure. The significance of the study is to extend existing knowledge of cybersecurity disclosure for large public companies and to present ideas for future research post 2018 SEC Commission's interpretive guidance.

The study uses 10-K information provided on companies listed on the Standard & Poor's list of the 500 large-cap American companies (S&P 500) to answer research questions related to the informativeness of cybersecurity risk disclosure, Specifically, the research questions test whether (1) the quantity of cybersecurity risk disclosure for S&P 500 companies has significantly improved in light of the SEC's new disclosure requirement, (2) any relationship exists between corporate 10-K cybersecurity disclosures and the number and type of cybersecurity breaches reported by the Privacy Rights Clearing House (PRC) and (3) specific variables such as company size, industry, breach type, and presence of prior or current year breach impact, the disclosure of cybersecurity breaches.

The literature review below provides information on the dearth of information published on cybersecurity disclosure. This study contributes to the literature on cybersecurity disclosure by providing insights into current disclosure practices and suggesting areas for future research.

The paper is organized as follows: in the following section we review studies published on cybersecurity and identify the research questions that are applicable to this study; in the subsequent section we discuss our research methodology including the sample selection and statistical analysis used and the results of our analyses are reported and discussed; finally, we conclude with a discussion including implications of our study, suggestions for future research and limitations.

LITERATURE REVIEW AND RESEARCH QUESTION DEVELOPMENT

Risk Factor Disclosure Studies

Beginning in 2005, the SEC required all public firms to include a Risk Factor section in their 10-K which discusses "the most significant factors that

could make the company speculative or risky" (SEC 2005). In 2011 and then again in 2018, the SEC issued additional Risk Factor guidance to all public firms regarding disclosure obligations relating to cybersecurity risks and cyber incidents. Included in this guidance is the requirement for registrants to disclose under Risk Factors in the 10-K, the risks the company faces in regards to cybersecurity incidents. Within this guidance, the SEC warns companies to "avoid generic boilerplate disclosure" (SEC 2018).

Previous studies have investigated Risk Factor content in the annual report. Campbell, Chen, Dhaliwal, Lu & Steele (2014) examine information content of risk factor disclosures following the 2005 SEC ruling by analyzing 10-K reports downloaded from the Edgar database. They find that firms with more risk exposure disclose more risks and the type of risk determines how much content is included to describe that risk. In addition, they suggest that disclosures are not boilerplate but instead are firm specific and useful to investors. Wang, Kannan & Ulmer (2013) find that disclosed risk factors with "risk-mitigation themes" are less likely to be related to future breach announcements. Similarly, Li, No & Wang (2018) find that the association between the presence of cybersecurity risk disclosure and subsequently reported cybersecurity incidents become insignificant after the passage of the 2011 cybersecurity guidance.

Other descriptive studies suggest that the 2011 guidance underachieves. Using case studies and SEC comment letters, Ferraro (2014) suggests that the guidance underachieves because it is "vague, similar across industries and companies, and bring little information to the marketplace" thus it fails to resolve the information symmetry problem it was aimed at correcting. In a Harvard Law School Forum investigating cybersecurity risk disclosures of Fortune100 companies following the 2011 SEC staff guidance, the post revealed that the depth and nature of cybersecurity disclosures varied greatly suggesting that there is still much room for improvement on cybersecurity risk disclosure (Klemash, Brorsen & Seets 2017).

The 2011 SEC staff guidance was issued with the goal of increasing cybersecurity risk disclosures by public companies. The guidance specifically states that *material* cybersecurity risks and incidents must be disclosed in the 10-K. Studies have shown that companies underreport events particularly due to alternative interpretations of the definition materiality (Young 2013).

To date, there have been no empirical studies investigating the link between reported cybersecurity incidents and risk factor disclosures. In light of the increasing scrutiny of cybersecurity disclosures by the SEC of public companies with reported breaches (e.g. Amazon and Google) there is a need for studies investigating cybersecurity disclosures in public company filings. The

following section identifies the importance of cybersecurity disclosure research and presents the research questions addressed in the study.

Research Question Development

Although there are no formal SEC rules or regulations addressing cybersecurity disclosure, a number of existing disclosure requirements may impose an obligation on registrants to disclose such risks and incidents. For example, the SEC Act of 1933 includes Item 503(c) of Regulation S-K, which requires public companies to disclose "the most significant factors that may adversely affect the issuer's business, operations, industry or financial position or its future financial performance" (SEC 1933). The SEC Act of 1934 requires publicly traded companies to report certain "material events" to shareholders in the Form 8-K if "deemed important to shareholders" (SEC 1934). Beginning in 2005, the SEC mandated all public companies to include a "risk factor" section in their annual 10-K" (SEC 2005) and in 2011, the SEC issued new risk factor disclosure obligations that focus on cybersecurity risks specifically (SEC 2011).

The 2011 SEC guidance is consistent with other disclosure requirements mandated by federal securities laws associated with any significant business risk. However, the risks associated with cybersecurity go beyond generic risks that could apply to all SEC registrants. The new guidance suggests disclosures should focus on the unique facts and circumstances related to specific, material cybersecurity risk. In light of the increase in cyber incidents to public companies and the requirement to disclose material cyber incidents in the 10-K we would expect cybersecurity risk factor disclosure to increase since the 2011 guidance release. Which leads to research question one:

> **RQ1:** Have cybersecurity risk factor disclosures in the *Risk Factors* section of the annual 10-K increased after the SEC issued the disclosure guidance?

Prior studies on corporate disclosure suggest that managers have a self-serving bias to disclose favorable information about the firm (Campbell et al. 2014) and are likely biased against providing unfavorable disclosures (Kothari, Li & Short 2009). Since risk factor disclosure such as those provided on cybersecurity are designed to relay information regarding unfavorable risks and uncertainties of the firm, it is likely that the SEC guidance on cybersecurity disclosures may prompt managers to provide vague and/or *boilerplate* disclosures. For example, according to the Privacy Rights Clearinghouse (PRC 2018), Yahoo has incurred several data breaches between 2012 and 2016. In 2013 it suffered a data breach originally estimated to impact 1 billion users (in 2017 Yahoo upped this estimate to 3 billion), in 2014 it suffered yet another data breach impacting over 500 million users and in 2017 it warned of an ongoing investigation that

impacted its 2015 and 2016 customers). In Yahoo's 2013, 2014, and 2015 10-K filings, although they include a cybersecurity risk factor, they fail to provide any information on the actual data breaches they incurred. Instead, the risk factor provided in the 10-k for all 3 years is a boilerplate disclosure that reads:

> ***Interruptions, delays, or failures in the provision of our services could damage our reputation and harm our operating results.***
>
> *Delays or disruptions to our service, or the loss or compromise of data, could result from a variety of causes, including the following:*
>
> • *Our operations are susceptible to outages and interruptions due to fire, flood, earthquake, tsunami, other natural disasters, power loss, equipment or telecommunications failures,* ***cyber attacks****, terrorist attacks, political or social unrest, and other events over which we have little or no control. We do not have multiple site capacity for all of our services and some of our systems are not fully redundant in the event of delays or disruptions to service, so some data or systems may not be fully recoverable after such events.*
>
> ***If our security measures are breached, our products and services may be perceived as not being secure, users and customers may curtail or stop using our products and services, and we may incur significant legal and financial exposure.***
>
> *Our products and services involve the storage and transmission of Yahoo's users' and customers' personal and proprietary information in our facilities and on our equipment, networks and corporate systems.* ***Security breaches expose us to a risk of loss of this information, litigation, remediation costs, increased costs for security measures, loss of revenue, damage to our reputation, and potential liability……... If an actual or perceived breach of our security occurs****, the market perception of the effectiveness of our security measures could be harmed and we could lose users and customers* (Yahoo 2013, 2014, 2015).

It is not until the 2016 that Yahoo actually identifies in its 10-K that it had a data breach and it only highlights the 2014 incident with no specific details relating to the number of customers impacted or the cost of the breach.

> ***Our security measures may be breached as they were in the Security Incidents and user data accessed, which may cause users and customers to curtail or stop using our products and services, and may cause us to incur significant legal and financial exposure.***
>
> *Our products and services involve the storage and transmission of Yahoo's users' and customers' personal and proprietary information in*

> *our facilities and on our equipment, networks, and corporate systems.* ***Yahoo is routinely targeted by outside third parties,*** *including technically sophisticated and well-resourced state-sponsored actors, attempting to access or steal our user and customer data or otherwise compromise user accounts.* ***We believe such a state-sponsored actor was responsible for the theft involved in the 2014 Security Incident****……..We take steps to prevent unauthorized data disclosure or access to our systems; however, because the techniques used to obtain unauthorized access, disable or degrade service, or sabotage systems change frequently or may be disguised or difficult to detect, or designed to remain dormant until a triggering event, we may be unable to anticipate these techniques or implement adequate preventative measures. Breaches of our security measures, such as the Security Incidents, or perceived breaches, have caused and may in the future cause, the market perception of the effectiveness of our security measures to be harmed and could cause us to lose users and customers, or detrimentally affect our relationships with distribution partners, service providers, vendors and app developers* (Yahoo 2016).

Interestingly, the SEC's first enforcement order issued in April 2018 was against Yahoo for failure to disclose a material cybersecurity breach and this order has some common links with the new cybersecurity guidance that was issued in 2018 (SEC 2018a). For example, the new guidance stresses the importance of board risk oversight and specifically states that "the risk management process should provide important information to investors about how a company perceives the role of its board and the relationship between the board and senior management in managing the material risks facing the company" (SEC 2018). In the order against Yahoo, the SEC found that the company's "risk factor disclosure in its annual and quarterly reports from 2014 through 2016 were materially misleading in that they claimed the company only faced the risk of potential future breaches" (SEC 2018a) when in fact a massive data breach had already occurred. In addition, the SEC found that Yahoo's senior management and legal teams did not share information regarding the data security breach with Yahoo's outside auditors or outside counsel (SEC 2018a).

Similarly, Amazon incurred a data breach in 2011 caused by a password security flaw. In Amazon's 2011 10-K filings, there is no mention of the breach. Instead, the risk factor provided in the 10-k is a boilerplate disclosure that reads:

> ***We Could Be Harmed by Data Loss or Other Security Breaches***
>
> *As a result of our services being web-based and the fact that we process, store and transmit large amounts of data, including personal information, for our customers, failure to prevent or mitigate data loss or other* **security breaches**

> **could expose us or our customers to a risk of loss or misuse of such information, adversely affect our operating results, result in litigation or potential liability for us and otherwise harm our business.** *Although we have developed systems and processes that are designed to protect customer information and prevent data loss and other security breaches, such measures cannot provide absolute security. In addition, we rely on third party technology and systems in certain aspects of our businesses, including for encryption and authentication technology to securely transmit confidential information* (Amazon 2011).

Home Depot also suffered a breach in 2010 as a result of credit card information being stolen via a skimming device. In Home Depot's 2010 10-K filings, there is no mention of the breach. Instead, the risk factor provided in the 10-K is a boilerplate disclosure that reads:

> ***If we do not maintain the security of customer, associate or company information, we could damage our reputation, incur substantial additional costs and become subject to litigation.***
>
> ***Any significant compromise or breach of customer, associate or company data security could significantly damage our reputation and result in additional costs, lost sales, fines and lawsuits****. The regulatory environment related to information security and privacy is increasingly rigorous, with new and constantly changing requirements applicable to our business, and compliance with those requirements could result in additional costs. There is no guarantee that the procedures that we have implemented to protect against unauthorized access to secured data are adequate to safeguard against all data security breaches* (Home Depot 2010).

The SEC guidance clearly states that "registrants should provide disclosure tailored to their particular circumstances and avoid generic boilerplate disclosure" (SEC 2011). However, these generic cybersecurity risk factor disclosures are clearly not informative about Yahoo's, Amazon's or Home Depot's specific cybersecurity risks. Instead, it illustrates that cybersecurity risk factor disclosures are used to highlight all possible risks and uncertainties regardless of the likelihood that they will impact the firm. Similar examples of boilerplate cybersecurity disclosures can be found in many other corporate filings (e.g. Best Buy, McDonalds, Lockheed Martin, Netflix, etc.).

Companies have many reasons for not disclosing cyber incidents (reputation, brand strength, market position, ability to raise capital, etc.). However, companies may face legal incentives to provide meaningful, firm specific cybersecurity risk factors particularly if a known material cybersecurity risk comes to light. If companies fail to disclose the known cybersecurity risk,

they could face sanctions by the SEC. For example, in 2012, the SEC sent letters to six companies (Amazon.com, American International Group Inc. (AIG), Eastman Chemical Co., Google, Hartford Financial Services Group Inc., Quest Diagnostics Inc.) identifying inadequacies of cybersecurity risk disclosures in their annual reports. The SEC determined that these firms did not go far enough to inform investors of the risk of cyber-attacks and did not disclose the fact that such attacks had occurred (Ferraro 2014). For example, Amazon's risk factor reported in their 2011 10-K read:

> ***We Could Be Liable for Breaches of Security***
> *……Although we have developed systems and processes that are designed to protect customer information and prevent fraudulent transactions, data loss and other security breaches, failure to prevent or mitigate such breaches may adversely affect our operating results* (Amazon 2011).

In the SEC comment letter to Amazon, the SEC asks Amazon to explain their cybersecurity risk factor disclosure as it relates directly to the 2011 guidance "in light of the fact that your subsidiary [Zappos] has actually experienced this cyber attack" (SEC 2012). At first Amazon protested claiming that "information on the specific incident would not provide investors with additional material information relating to the cyber-attack risks" (SEC 2012). After persistence from the SEC, Amazon was compelled to change their cybersecurity risk factor in 2013 addressing the fact that some its subsidiaries had past security breaches.

> ***We Could Be Harmed by Data Loss or Other Security Breaches***
> *……We use third party technology and systems for a variety of reasons, including, without limitation, encryption and authentication technology, employee email, content delivery to customers, back-office support, and other functions.* ***Some subsidiaries had past security breaches, and, although they did not have a material adverse effect on our operating results, there can be no assurance of a similar result in the future.*** *Although we have developed systems and processes that are designed to protect customer information and prevent data loss and other security breaches, including systems and processes designed to reduce the impact of a security breach at a third party vendor, such measures cannot provide absolute security* (Amazon 2013).

Thus, in light of the importance that the SEC is placing on cybersecurity risks disclosure and the SEC's disclosure guidance published in 2011, it would be expected that corporate filers would be more cognizant of providing firm specific cybersecurity risk factor disclosure in their 10-K particularly when the firm has a reported cybersecurity breach in the same year. Which leads to our second research question:

RQ2: Are companies that have reported cybersecurity breaches (as documented by the PRC) prior to or in the year of the SEC disclosure guidance, more likely to provide a cybersecurity risk factor in the 10-K under risk factors?

With the pervasiveness of technology, material cyber incidents pose a threat to all companies regardless of industry. Some industries may be at a higher risk than others particularly if they gather personally identifiable information. Beyond the SEC requirements, some industries have other regulatory bodies requiring disclosure for certain types of breaches (e.g. Health Insurance Portability and Accountability Act (HIPAA) for healthcare companies, Payment Card Industry Data Security Standard (PCI-DSS) for retailers, etc.). Thus, our third and fourth research question investigates whether type of breach or industry has an impact on cybersecurity risk factor disclosure.

RQ3: Does the type of reported cybersecurity breach (as documented by the PRC) have an impact on cybersecurity risk factor disclosure in the annual 10-K?

RQ4: Does the industry in which the company operates (using the SEC SIC codes) have an impact on cybersecurity risk factor disclosure in the annual 10-K?

DATA AND METHODOLOGY

Sample and Data

Our sample uses companies listed on the S&P 500. We obtain financial statement data from S&P's Research Insight (i.e., Compustat). Security breach data is collected on these companies from the Privacy Rights Clearinghouse (PRC) website (privacyrights.org). The PRC is a nonprofit corporation that reports data security breaches made public since 2005. The database compiles breach information from various governmental agencies and other verifiable media sources such as Open Security Foundation list-serve, Databreaches.net, Personal Health Information (PHI) Privacy, National Association for Information Destruction (NAID) and the California Attorney General.

We identify firms involved in breaches reported by the PRC and match these firms to our list of S&P 500 firms. We manually collected for each data breach, the type of breach (as identified by the PRC - hacking or malware, unintended disclosure, payment card fraud, insider, physical loss, etc.), date of breach, information source, estimated cost of the breach and other relevant information. We match the reported data security breaches to companies listed on

the S&P 500. We then collect cybersecurity and data breach disclosure data from SEC financial filings in the 10-K both pre and post the issue date of the SEC disclosure guidance by performing content analysis. We eliminated 87 S&P 500 firms with missing financial data in one or both of the 10-Ks, yielding a sample size of 413 firms. Table 1, Panel A below presents the demographics of the sample. Manufacturing represents the largest portion of the sample (160 companies 39 percent) followed by Finance (69 companies 17 percent) and Services (49 companies 12 percent). The average size of the firms measured by total assets for 2010 (2011) is $12,179 ($14,138) million.

Table 1
Panel A: Sample data by industry

Industry	**N**	**%**	**Average Total Assets ($Millions)**	
			2010	**2011**
Mining	30	7%	18,368	20,562
Construction	4	1%	5,521	6,221
Manufacturing	160	39%	24,248	25,986
Transportation, Communication, Electric, Gas & Sanitary Services	61	15%	33,286	33,336
Wholesale & Retail Trade	40	10%	16,571	17,816
Finance, Insurance & Real Estate	69	17%	192,126	197,579
Services	49	12%	13,725	15,255
Total	413	100%	51,030	53,090
Median			12,719	14,138

Cybersecurity Risk Factor Frequency Analysis for RQ1

Cybersecurity incidents pose threats that not only the affect public corporations but also investors and the capital markets. The SEC, highlighting the importance of cybersecurity risk disclosure, issued a guidance in 2011 prompting public companies to be more forthcoming when disclosing cybersecurity risks. The SEC's guidance focused on addressing discrepancies in disclosure practices among public companies. Thus, we would expect cybersecurity risk factor disclosures to increase as a result of the 2011 guidance. Therefore, for RQ1, we examine whether cybersecurity risk factor disclosures increased after the SEC issued the disclosure guidance.

We explore RQ1 by performing content analysis. Content analysis is a research technique for "making replicable and valid inferences from tests (or other meaningful matter) to the context of their use" (Krippendorff, 2004, pg. 18). Content analysis is considered appropriate for the analysis of companies' annual reports (Beretta & Bozzolan 2004; Linsley & Shrives 2006). We do a keyword search for any/all references to cybersecurity (e.g. cybersecurity, cyber-security, cyber-attack, data security, information security, security breach, breach, security, security incident, etc.) and document where and how it is reported in the 10-K.

Table 2 below shows the number of S&P 500 companies disclosing a cybersecurity risk factor in their 10-K during periods before (2010) and after (2011) the date of the SEC guidance. Results show that during this period, cybersecurity risk disclosures in the *risk factor* section of the 10-K increased by 23 percent for our sample. In 2010, there were 188 (46 percent) organizations that included a cybersecurity risk factor in their 10-K and in 2011 there were 283 (69 percent) organizations.

Table 2
Companies disclosing a cybersecurity risk factor pre and post SEC CF Disclosure Guidance: Topic No. 2 – Cybersecurity.

Fiscal Year	N	Cybersecurity Risk Factor Disclosure	Mean	StdDev	Min	Max
2010	413	188 46%	0.455	0.498	0	1
2011	413	283 69%	0.685	0.465	0	1

***** t-test, increase in number of companies providing cybersecurity risk factor disclosure significant at p <0.000 (*t=10.049); Mann Whitney U test significant at p<0.000 (z=6.673)*

These results suggest that the 2011 guidance, issued by the staff, does not go far enough to encourage disclosure and shows that public companies are underreporting cybersecurity incidents (note that "staff statements are nonbinding and create no enforceable legal rights or obligations of the Commission or other parties" but are important in the development of rules and regulations issued by the SEC Commission) (Clayton 2018). However, the 2011 guidance was considered necessary because at that time it was issued, there were no existing disclosure requirements addressing cybersecurity specifically. More recently, in 2018 the SEC voted to approve a statement and interpretive guidance on public

company cybersecurity disclosures. The 2018 guidance, issued by the commission itself, carries more weight (note that only the SEC Commission has the ability to "adopt rules and regulations that have the force and effect of law") (Clayton 2018), than the 2011 staff guidance. The Commission's guidance addresses specific criteria for determining whether a breach is *materia*l, discussions on timing of when a breach should be disclosed and board oversight responsibilities. The goal of the guidance is to promote "clearer and more robust disclosure by companies about cybersecurity incidents, resulting in more complete information being available to investors" (SEC adopts 2018).

With the release of this new guidance, future research could investigate whether the clarifications provided in the 2018 interpretive guidance has had a meaningful impact on corporate cybersecurity disclosure tendencies post issuance. In particular, future studies could investigate how the 2018 guidance influenced the interpretation of materiality by corporate filers (including an analysis of the probabilities used to assess the likelihood of an incident occurring), the timeliness and the specific details disclosed following a breach, changes in cybersecurity risk factor disclosures (ensuring companies are providing specific details instead of merely boilerplate disclosures) and changes to corporate governance procedures as they relate to the mitigation of cybersecurity risks.

Cybersecurity Risk Factor Disclosure Determinant Analysis for RQ2

Next, we use our sample firms and match them against the list of public companies that have suffered a data security breach as reported by the PRC. The PRC has been tracking data breaches made public (via newspapers and other media) since 2005 and this report is available to the public. Using this report, for RQ2, we explore whether firms that have had a prior data security breach are more likely to disclose a cybersecurity risk factor in their 10-K.

Table 3 below provides descriptive details on the actual number of breaches and disclosure information for our sample years. For 2010, we determined that 33 (8 percent) organizations from our sample had documented breaches. Of those 33, 18 (55 percent) included a cybersecurity risk factor in their annual 10-K and none provided disclosure of the actual breach anywhere within the 10-K. For 2011, we determined that 29 (7 percent) organizations from our sample had documented breaches. Of those 29, 19 (66 percent) included a cybersecurity risk factor in their annual 10-K.

Of those organizations in 2011 that had a reported breach, 2 (7 percent) disclosed actual information regarding the breach in their annual 10-K. EMC Corporation reported the breach in their cybersecurity risk factor, the results of

operation and the notes to the financial statements (included in the footnote was a customer remediation charge of $66.3 million). Note that the breach was related to their RSA Information Security Segment. Fidelity National Information Service, Inc. reported the breach in the business section, cybersecurity risk factor and the notes to the financial statements (included in the footnote was an estimated loss of $13 million related to the breach).

Table 3
Descriptives on actual breach data as reported by the PRC.

Fiscal Year	N	Total Number of Reported Breaches in Reporting Year	Number of Companies with Reported Breach with Cybersecurity Risk Factor Disclsoure	Number of Companies providing actual disclosure of breach	Total Number of Reported Breaches up to and including Reporting Year
2010	413	33 8%	18 55%	0 0%	144 35%
2011	413	29 7%	19 66%	2 7%	173 42%

We then explore RQ2 by examining whether the presence of a prior reported cybersecurity breach is related to the likelihood of a firm disclosing a cybersecurity risk factor in the 10-K by employing a binary logistic model. Classical linear regression models are not valid for binary dependent variables. Logistic regression (developed by David Cox in 1958) allows us to estimate the odds of a binary outcome based on one or more explanatory variables. Peng, So, Stage & St John (2002) suggest a minimum number of observations for logistic regression should be about 100; therefore, our sample size of 413 is adequate for this methodology. Our model for RQ2 includes measures of size, presence of a prior year breach and presence of a current year breach.

We estimate the following binary logistic regression model to investigate RQ2:

$$DISCL = a_1 + \beta_1 (SIZE) + \beta_2 (PRIORBREACH) + \beta_3 (CURRENTBREACH)$$

Where the dependent variable DISCL is a binary indicator variable equal to 1 if the company included a cybersecurity risk factor in the current fiscal year and 0 otherwise; SIZE is a control variable measured by the log of total assets; PRIORBREACH is an indicator variable equal to 1 if the firm had a prior reported breach as reported by PRC (between 2005 and 2009), or otherwise 0; CURRENTBREACH is an indicator variable equal to 1 if the firm had a reported breach in the reported year (2010 or 2011), or otherwise 0.

We report descriptive statistics for the variables used to conduct our test of RQ2 in Table 4, Panel A (B) of Table 4 reports various univariate descriptive statistics for year 2010 (2011) of our sample. To test the determinants of disclosure, we used binary logistic regression. Table 4, Panel C presents the correlations of the variables under study.

Table 4

Panel A: 2010 Sample Descriptive Statistics

(n=413)

Variable	Mean	Median	StnDev
DISCL	0.455	0.000	0.498
SIZE (LogTA)	4.185	4.113	0.624
CURRENTBREACH	0.030	0.000	0.171
PRIORBREACH	0.088	0.000	0.284
TYPE	3.878	3.000	2.177
INDUSTRY	4.162	4.000	1.701

Table 4

Panel B: 2011 Sample Descriptive Statistics (n= 413)

Variable	Mean	Median	StnDev
DISCL	0.685	1.000	0.464
SIZE (LogTA)	4.262	4.156	0.826
CURRENTBREACH	0.027	0.000	0.164
PRIORBREACH	0.101	0.000	0.032
TYPE	4.206	4.000	1.739
INDUSTRY	4.162	4.000	1.701

Table 4

Panel C: Correlations Table

	DISCL	PRIOR BREACH	CURRENT BREACH	SIZE	TYPE	INDUSTRY
DISCL	1					
PRIOR BREACH	.187**	1				
CURRENT BREACH	0.046	-.105**	1			
SIZE	.094**	.173**	.135**	1		
TYPE	.190**	.598**	.498**	.297**	1	
INDUSTRY	.356**	.180**	.151**	0.067	.245**	1

**. Correlation is significant at the 0.01 level (2-tailed).

Table 5 presents the results of our binary logistic regression analysis for RQ2 on the choice to disclose a cybersecurity risk factor. We run this model for the year prior to the issuance of the guidance (2010) and the year of the guidance (2011). We used Wald statistics to test the significance of the Log Regression Coefficients for each of our independent variables.

As noted in Table 5 - Panel A, the results of the 2010 analysis indicate a positive and statistically significant (p=.012) relation between prior reported breaches and the choice to disclose a cybersecurity risk factor suggesting a higher propensity to disclose a cybersecurity risk factor disclosure in the 10-K if the organization had a prior reported cybersecurity breach. The SIZE of the company as measured by the log of total assets was marginally significant (p=.074) and PRIORBREACH was not significant.

Table 5
Panel A: Logistic Regression Analysis RQ2 (2010)

Independent Variables	**B**	**SE B**	**e^B**
SIZE (LogTA)	0.313*	0.175	1.367
CURRENTBREACH	0.767	0.480	2.152
PRIORBREACH	0.708**	0.283	2.031
Constant	-1.657		
$\chi 2$ = 19.915, p<.001 with df=3			
Cox & Snell R Square	0.047		
Nagelkerke R Square	0.063		

**p<.10, **p<.05, ***p<.01, ****p<.001*

Similarly, the results for 2011 as shown in Table 5 – Panel B indicate a statistically significant (p=.001) relation to prior reported breaches and the choice to disclose a cybersecurity risk factor where the log odds of a company reporting a cybersecurity risk factor was positively related to having a prior reported breach. These results may provide an indication that the 2011 Cybersecurity Guidance is having a positive and significant impact as more companies that have suffered a cybersecurity breach in the past are including in their disclosures a cybersecurity risk factor. However, beyond the risk factor section, specific disclosures related to an actual security breach remains insufficient. The SIZE of the company and having a current year breach was not significant.

Table 5
Panel B: Logistic Regression Analysis RQ2 (2011)

Independent Variables	B	SE B	e^B
SIZE (LogTA)	-0.020	0.139	0.980
CURRENTBREACH	0.532	0.584	1.703
PRIORBREACH	1.063****	0.330	2.894
Constant	0.661		
$\chi 2$ = 14.737, p<.01 with df=2			
Cox & Snell R Square	0.042		
Nagelkerke R Square	0.056		

**p<.10, **p<.05, ***p<.01, ****p<.001*

The results showing that size does not influence disclosure is not surprising, as prior research shows, public companies underreport events due to alternative interpretations of the definition of materiality (Young 2013). Young argues that without further guidance on what constitutes a material event, it is not surprising the materiality threshold remains subjective. In addition, there is a reluctance by public companies to report security breaches for fear of alarming stakeholders and possibly affecting stock prices. Without regulations enforcing disclosure, it is likely that this trend will persist.

The findings that companies with a prior reported breach are more likely to include a cybersecurity risk factor is of interest and the fact that the significance is much stronger in 2011 may suggest that the guidance is influencing disclosure. Since materiality must be considered throughout the cybersecurity disclosure decision, future research should investigate the best way to define materiality to see if there are any measures that could best be used to determine when a material cybersecurity breach must be disclosed.

Young (2013) proposes that the SEC "should institute dollar and percentage of assets thresholds for determining materiality." Following Young, future research should investigate legal proceedings issued referencing materiality (e.g. references to Regulation S-K) to determine how materiality has been defined in the courts and use this information to develop a materiality framework that would help eliminate inconsistencies in the interpretation of materiality. Future research could also investigate public company cybersecurity incident disclosure based not only on quantitative factors (some cybersecurity incidents are so large and impactful, disclosure is unavoidable – Anthem, JPMorgan Chase, Home Depot, Target, Sony, etc.) but also on qualitative factors which are more difficult to measure (e.g. reputation damage and loss of consumer confidence).

Cybersecurity Risk Factor Disclosure Determinant Analysis for RQ3

We next investigate whether the type of breach has an impact on risk factor disclosure. For RQ3, we explore whether the type of reported cybersecurity breach is related to the likelihood of a firm disclosing a cybersecurity risk factor. We use PRC's data breach classifications. The classifications include: Payment Card Fraud (CARD) this involves debit and credit card fraud; Hacking or Malware (HACK) this involves fraud as a result of an outside party or malware; Insider (INSD) this involves fraud from someone with legitimate access; Physical Loss (PHYS) this includes paper documents that are lost or stolen; Portable Device (PORT) this includes lost, discarded or stolen physical devices (i.e. laptop, PDA, smartphone, etc.); Stationary Device (STAT) this includes non-mobile devices; Unintended Disclosure (DISC) this includes fraud not involving hacking, intentional breach or physical loss (e.g. sensitive information posted publicly, mishandled electronic information, etc.); and Unknown (UNKN).

We estimate the following binary logistic regression model to investigate RQ3:

$$DISCL = a_1 + \beta_1 (SIZE) + \beta_2 (TYPE)$$

Where TYPE is a categorical variable ranging from 1 to 8. Using TYPE as part of this exploratory research is particularly useful in identifying trends and in establishing benchmarks for future comparison. We run this model for the year prior to the issuance of the guidance (2010) and the year of the guidance (2011). Table 6 presents the results of our binary logistic regression analysis for RQ3. We used Wald statistics to test the significance of the Log Regression Coefficients for each of our independent variables.

Table 6, Panel A provides details on the TYPE of breach by year (2005-2011) for our sample companies as reported by the PRC. Trends show that from 2005 through 2009 that breaches classified as PORT made up the majority of the reported breaches (ranging from 15 percent to 63 percent). In the years 2010 breaches classified as INSD and DISC made up the majority of the reported breaches (21 percent and 33 percent respectively) and in 2011 breaches classified as HACK, PORT and STAT made up the majority of the breaches (21 percent, 21 percent and 34 percent respectively).

Table 6
Panel A:
Breakdown of TYPE of breach by year

TYPE	2005	2006	2007	2008	2009	2010	2011	Total
CARD	0	0	0	1	2	2	4	9
HACK	1	2	2	2	2	6	10	25
INSD	0	5	5	2	4	11	3	30
PHYS	0	1	0	2	0	4	6	13
PORT	7	18	19	8	2	1	0	55
STAT	1	3	1	2	0	0	6	13
DISC	3	5	3	1	3	7	0	22
UNKN	0	3	0	1	0	2		6
Total	12	37	30	19	13	33	29	173

Table 6, Panel B presents the results of our RQ3 analysis. For 2010, the results show that the log of the odds of a company disclosing a cybersecurity risk factor was positively and significantly related to breaches classified as HACK (electronic entry by an outside party, malware or spyware) (p=.019) suggesting a higher likelihood to disclose a cybersecurity risk factor disclosure in the 10-K. SIZE was also positively and significantly associated with the likelihood to disclose a cybersecurity risk factor (p=.049).

Breaches classified as CARD, INSD, PHYS, PORT, STAT and DISC were not factors in predicting disclosure. Hacking is one of the most common methods used by thieves to steal personally identifiable information, so it is not surprising that breaches classified as HACK had a positive and significant impact on cybersecurity risk disclosure.

Table 6
Panel B: Logistic Regression Analysis RQ3 (2010)

Independent Variables	B	SE B	e^B
SIZE (LogTA)	0.363**	0.184	1.438
CARD	0.215	1.293	1.239
HACK	2.487**	1.058	12.029
INSD	0.723	0.587	2.061
PHYS	-1.860	0.794	0.830
PORT	0.201	0.365	1.223
STAT	-1.261	1.074	0.283
DISC	0.455	0.601	1.576
Constant	-1.804		
$\chi 2$ = 25.302, p<.001 with df=8			
Cox & Snell R Square	0.059		
Nagelkerke R Square	0.079		

**p<.10, **p<.05, ***p<.01, ****p<.001*

For 2011 (Table 6 – Panel C), breaches classified as DISC (sensitive information posted publicly on a website, mishandled, or sent to the wrong party via e-mail, fax, or mail) were marginally significant (p=.074) suggesting a higher likelihood to disclose a cybersecurity risk factor disclosure in the 10-K. However, the size of the organization as well as breaches classified as INSD, PHYS, PORT and STAT were not factors in predicting disclosure.

Table 6
Panel C: Logistic Regression Analysis RQ3 (2011)

Independent Variables	B	SE B	e^B
SIZE (LogTA)	-0.015	0.142	0.985
INSD	0.650	0.664	1.915
PHYS	-0.453	0.676	0.636
PORT	0.630	0.417	1.878
STAT	0.902	1.105	2.464
DISC	1.893*	1.058	6.641
Constant	0.704		
$\chi 2$ = 15.051 p<.05 with df=6			
Cox & Snell R Square	0.036		
Nagelkerke R Square	0.050		

**p<.10, **p<.05, ***p<.01, ****p<.001*

Cybersecurity Risk Factor Disclosure Determinant Analysis for RQ4

Our final analysis looked at disclosure relative to industry type. For RQ4 we review cybersecurity risk factor disclosures by looking for certain industry-specific trends. We estimate the following binary logistic regression model to investigate RQ4:

$$DISCL = a_1 + \beta_1 (SIZE) + \beta_2 (INDUSTRY)$$

Where INDUSTRY is a categorical variable ranging between 1 and 8 based on SIC codes as reported by the SEC (see Table 1 for industry descriptive statistics). Results (not tabulated) indicated that for 2010 and 2011 companies classified as Wholesale & Retail Trade and Services were positively and significantly related to disclosure of cybersecurity risk factors (p=.001 and p=.000 respectively; p=.048, p=.077 and p=.001 respectively) suggesting a higher likelihood to disclose a cybersecurity risk factor disclosure in the 10-K. These results may be related to data breach notification laws directly affecting retailers, particularly as it relates to the handling of consumer data.

For 2010 and 2011 Companies classified as Manufacturing were negatively and significantly related to disclosure of cybersecurity risk factors (p=.000). Note that a large percentage of our sample size represents manufacturing firms (39%). Cyber-attacks against manufacturing firms are on the rise; this in part may be the result of companies in this industry not upgrading their overall cyber security systems thus becoming an easier target. Overall, all firms have an incentive not to disclose damages suffered from a data breach because 1)there are no specific reporting regulations requiring disclosure and 2) due to concerns of possibly turning away potential or existing customers, litigation and damaging their reputation or stock value.

Some industries may be more susceptible to cybersecurity breaches than others. The IBM 2016 Cyber Security Intelligence Index ranked healthcare organizations as number one for reported breaches followed by manufacturing firms, financial services, and government and transportations firms (2019 IBM X-Force 2019). The healthcare sector maintains a large amount of personal information (e.g., name, social security number, payment information etc.) that criminals consider valuable, therefore, it is not surprising that healthcare organizations are a prime target. In addition, manufacturers are often the target of cyber-attacks as many facilities use dated legacy equipment that were not designed with security in mind. Although all industries are vulnerable to cyber-attacks, some industries may be more susceptible than others. Thus, including INDUSTRY as part of this exploratory research is particularly useful in identifying trends and in establishing benchmarks for future comparison. As industries have different cybersecurity risk factors, future research should

investigate cybersecurity incident disclosure from an industry standpoint and compare/contrast the variables that prompt disclosure.

DISCUSSION, FUTURE RESEARCH AND LIMITATIONS

"Given the frequency, magnitude and cost of cybersecurity incidents" on public companies, the SEC was compelled to take actions to protect investors (SEC 2018). As a first step, the SEC staff issued a guidance in 2011 addressing the actions that public companies should take to inform investors about material cybersecurity risks and incidents. More recently, on February 26, 2018, the SEC Commission issued interpretive guidance to aid public companies with their cybersecurity disclosures. It is important to note that both guidance advisories target not only companies that have suffered a cybersecurity breach but also those that might be subject to material cybersecurity risks. This study examined the impact of the SEC's 2011 guidance on cybersecurity risk factor disclosures. The results suggest that companies seem to have responded cautiously to the SEC's 2011 Cybersecurity Risk Factor Guidance. For our sample companies, there was an overall 23 percent increase in the number of organizations that included a cybersecurity risk factor in their annual 10-K report after the SEC issued its disclosure guidance. Factors that influenced disclosure included the size of the organization, whether the firm had any prior reported breaches as documented by the PRC and type of breach. Of particular interest to this study is the lack of disclosure in the narrative of the 10-K by companies that have suffered an actual breach. From our sample companies, only two companies in 2011 that had a reported breach actually disclosed information on the breach in their annual 10-K.

As the SEC ramps up its investigations of public companies for insufficient disclosure of cybersecurity risks and actual breaches through enforcement actions and comment letters, it presents an opportunity for future research. Throughout this manuscript, we have addressed several areas that warrant future research relating to cybersecurity disclosure. Next, we present some additional suggestions for future research in this area.

Future research should include descriptive studies that examine the issues identified in the SEC's enforcement actions and comment letters and compare these to the advice provided in the cybersecurity guidance. As noted previously, there is a certain level of consistency between the issues identified in the Yahoo enforcement order and the 2018 SEC cybersecurity guidance. Given that the CEO and CFO have to certify the effectiveness of the internal controls and the adequacy of controls and procedures for identifying cybersecurity risks and incidents, the findings of such a study should of interest to public companies

particularly as they reevaluate they cybersecurity risk profile and ramp up their board risk oversight on cybersecurity.

Similarly, future research should address questions that Board of Directors (BOD) will face regarding their roles and responsibilities for cybersecurity. For example, how does the SEC cybersecurity guidance impact board risk oversight? Are the BOD's formally assigning responsibility for cybersecurity at both the board and the management level? Do the BOD have access to cybersecurity experts? Do the company's disclosure controls and procedures provide for an early warning system when a breach occurs? Does the board understand how cybersecurity risks integrate into the company's overall risk management programs? How will the SEC cybersecurity guidance and investor interest impact future cybersecurity risk disclosures?

As the SEC moves towards a cybersecurity disclosure *regulation* (versus a guidance) for reported events of information security breaches, more information is needed to identify the strengths and weaknesses of current disclosure tendencies. This study is the first step in identifying how organizations are currently reporting 1) the risk of cybersecurity breaches and 2) the actual details of cybersecurity breaches. Future research should investigate cybersecurity disclosures behavior post 2018 Commission guidance based on general deterrence theory. General deterrence theory suggest that the perceived likelihood of being caught and the perceived severity of the punishment are likely to be key decision factors for disclosure. Unless some legal action is initiated by the SEC (through regulation) or by stockholders for underreporting cybersecurity risks, it is likely that cybersecurity risks/breaches will go unreported. Although the 2011 staff guidance poses no risk of punishment for underreporting cybersecurity, the 2018 guidance may prompt the SEC to issue sanctions against public companies. Cybersecurity disclosure remains one of the hot topics for the SEC.

Future research should also include contextual studies looking specifically at cybersecurity risk factor disclosures to determine whether the information provided by organizations are informative or merely *boilerplate* paying close attention to those firms that have suffered an actual breach as reported by the PRC. Other studies may investigate the intentional underreporting of cybersecurity events resulting from agency theory - as it may be in the interest of management to understate cybersecurity risk particularly if the firm is performing poorly. Future studies on cybersecurity may also benefit by investigating whether a firm's disclosure practices are consistent with the actual cybersecurity it faces. This would involve interviewing management to better understand how a firm assesses cybersecurity threats and its disclosure decisions relating to both actual breach disclosures and future cybersecurity risk. Still other

behavioral research ideas could examine whether current disclosure is informative enough to aid in investor decision making.

It is important to note that public companies have requirements beyond the SEC guidance to disclose public breaches particularly when it involves consumer's personally identifiable information. Over 46 of the 50 US states currently have consumer protection laws requiring disclosures beyond the 10K. Most recently, the European Union (EU) issued the EU General Data Protection Regulation (GDPR). The regulation addresses data protection and privacy for all individuals within the EU as well as the export of personal data outside the EU. There are numerous laws protecting individuals' personal data (Gramm-Leach-Bliley Act, HIPAA, FTC, GDPR, etc.). Future research should investigate how these consumer protection laws influence corporate disclosure of cybersecurity incidents.

This study should be of interest to the SEC as Jay Clayton, chairman of the SEC acknowledged in a public statement on cybersecurity on Sept 20, 2017 that "cybersecurity is critical to investors, market participants our markets and the Commission itself." He went on to state that the commission "will continue to evaluate this [CF Disclosure] guidance…and its impacts on issues and capital markets (SEC Public Statement Clayton 2017)." The SEC cybersecurity guidance notes that material cybersecurity risks and incidents must be disclosed. The SEC chairman states that he expects companies to take seriously their obligation to disclose material information about cyber risks and events and as a result, he expects the SEC staff to comment more on cybersecurity disclosures over the next year (SEC Speech Clayton 2017). Therefore, with the increased focus by the SEC on cybersecurity and the recently issued guidance advisories, it is important to evaluate the adequacy of public company disclosures regarding cybersecurity particularly as it relates to investors.

As with all research, our study is not without limitations. The first limitation is with regards to the sample which includes only S&P 500 firms. Selecting S&P 500 firms results in a sample of large firms, thereby limiting the generalizability of the results to smaller firms. Future researchers are encouraged to replicate these results amongst a data set that includes both large and small firms. The second limitation is with regards to the usage of the PRC's breach dataset. We cannot be certain that the PRC has captured all breaches for companies identified in our sample. In addition, we rely on the 10K for breach disclosures reported by our sample companies, which may also be a limiting factor. Some companies may not disclose a breach if they are not required by law/regulations and/or because of negative implications to their stakeholders. As the SEC is moving towards disclosure regulations, future research could test the effectiveness of such regulations. Regardless of the aforementioned limitations,

we are confident that these limitations do not weaken our analysis or alter our study's findings.

REFERENCES

Amazon (2011, 2013). Form 10-K. Retrieved from: https://ir.aboutamazon.com/annual-reports

Beretta, S. & Bozzzolan, S. (2004). A framework for the analysis of firm risk communication. *The International Journal of Accounting*, 39 (1), 265-288.

Campbell, J., Chen, H., Dhaliwal, D., Lu, H. & Steele, L. (2014). The information content of mandatory risk factor disclosure in corporate filing, *Review of Accounting Studies,* 19 (396-455).

Chew, H. Newby, T, Fenwick & West (2017, November 20). Data breach settlements: Why are they getting Bigger? *Legaltechnews*. Retrieved from https://www.law.com/legaltechnews/sites/legaltechnews/2017/11/20/data-breach-settlements-why-are-they-getting-bigger/?slreturn=20190324103218.

Clayton, J. (2018, September 13). Statement regarding SEC staff views. *U.S. Securities and Exchange Commission*. Retrieved from https://www.sec.gov/news/public-statement/statement-clayton-091318.

Cox, D. (1958). The regression analysis of binary sequences. *Journal of the Royal Statistical Society. Series B (Methodological)*, 20 (2), 215-242.

Federal Trade Commission Act (FTC) (December 2016) Section 5: Unfair or deceptive acts or practices. Retrieved from https://www.federalreserve.gov/boarddocs/supmanual/cch/ftca.pdf.

Ferraro, M. (2014). "Groundbreaking" or broken? An analysis of the SEC cybersecurity disclosure guidance, its effectiveness and implications. *Albany Law Review*, 77.2, 297-347.

Giorgianni, A. (2017, September 17). Should you participate in a class action against Equifax? *Consumer Reports*. Retrieved from https://www.consumerreports.org/lawsuits-settlements/should-you-participate-class-action-against-equifax/.

Home Depot (2010). Form 10-K Annual Report. Retrieved from https://ir.homedepot.com/financial-reports/annual-reports/recent.

IBM X-Force Threat Intelligence Index (2019). *IBM.* Retrieved from https://www.ibm.com/security/data-breach/threat-intelligence.

Identity Theft Resource Center (ITRC) (2017). 2017 Annual Data Breach Year-End Review. Retrieved from www.idtheftcenter.org/2017-data-breaches.

Klemash, S., Brorsen, L. & Seets, C. (2018, October 21). Cybersecurity Disclosure Benchmarking. *Harvard Law School Forum on Corporate Governance and Financial Regulation*. Retrieved from https://corpgov.law.harvard.edu/2018/10/21/cybersecurity-disclosure-benchmarking/.

Kothari, S. P., Li, X., & Short, J. (2009). The effect of disclosures by management, analysts, and business press on cost of capital, return volatility, and analyst forecasts: a study using content analysis. *The Accounting Review*, 84, 1639–1670.

Krippendorff, K. (2004). Content Analysis: An introduction to its methodology (2nd ed.). Thousand Oaks, CA: Sage.

Linsley, P. & Shrives, P., (2006). Risk reporting: a study of risk disclosures in the annual reports of UK companies. *The British Accounting Review*, 38 (4), 387-404.

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

Muncaster, P. (2018, March 9). Yahoo agrees $80m securities class action settlement. *Information Security Magazine*. Retrieved from https://www.infosecurity-magazine.com/news/yahoo-agrees-80m-settlement/.

Peng, C. Y., So, T. S., Stage, F. K., & St. John, E. P. (2002). The use and interpretation of logistic regression in higher education journals: 1988-1999. *Research in Higher Education*, 43, 259-293.

Privacy Rights Clearinghouse (PRC) (2018). Data Breaches. Retrieved from https://www.privacyrights.org/data-breaches.

Rockefeller, J., Menedez, R., Whitehouse, S., Warner, M., & Blumenthal, R. (2011, May). "Letter from Five Senators to SEC Chairman Schapiro Regarding Cyber Security Disclosure." Retrieved from https://www.slideshare.net/100fsteet/letter-from-senator-rockefeller-to-sec-chairman-schapiro-regarding-cyber-security-disclosure-may-2011.

Rockefeller, J. (2013, April). "Letter from Rockefeller to SEC Chairman Schapiro Regarding Cyber Security Disclosure." Retrieved from https://www.commerce.senate.gov/public/_cache/files/49ac989b-bd16-4bbd-8d64-8c15ba0e4e51/B93E89CD80273341701DA31B2B6E1F6A.4-9-13-letter-to-chairman-white.pdf.

Sandler, L. (2012). Amazon, Google comply with SEC on cyberattacks. *The Seattle Times*, August 29, 2012.

Securities and Exchange Commission (SEC) Act of 1933 – Regulation S-K. Retrieved from https://www.ecfr.gov/cgi-bin/text-idx?amp;node=17:3.0.1.1.11&rgn=div5#se17.3.229_1503.

Securities and Exchange Commission (SEC) Act of 1934: Final Rule – Additional Form 8-K disclosure requirements and acceleration of filing dates. Release Nos. 33-8400; 34-49424; File No. S7-22-02. Retrieved from https://www.sec.gov/rules/final/33-8400.htm.

Securities and Exchange Commission (SEC) adopts statement and interpretive guidance on public company cybersecurity disclosures (2018, February 21). Securities and Exchange Commission [press release 2018-22]. Retrieved from https://www.sec.gov/news/press-release/2018-22.

Securities and Exchange Commission (SEC) Altaba, formerly known as Yahoo! (2018, April 24). Retrieved from https://www.sec.gov/news/press-release/2018-71.

Securities and Exchange Commission (SEC) Speech - Remarks at the Economic Club of New York by SEC Chairman Jay Clayton (2017, July 12). [Speech July 12, 2017]. Retrieved from https://www.sec.gov/news/speech/remarks-economic-club-new-york.

Securities and Exchange Commission (SEC) Public Statement on Cybersecurity by Chairman Jay Clayton (2017, September 20). Securities and Exchange Commission [public statement September 20, 2017]. Retrieved from https://www.sec.gov/news/public-statement/statement-clayton-2017-09-20.

Securities and Exchange Commission (SEC). (2005). Securities and exchange commission final rule, release no. 33–8591 (FR-75). Retrieved from http://www.sec.gov/rules/final/33-8591.pdf.

Securities and Exchange Commission (SEC). (2011). Securities and exchange commission guidance, CF Disclosure Guidance: Topic No. 2. Retrieved from http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

Securities and Exchange Commission (SEC) (2012). Correspondence to Amazon. Retrieved from https://www.sec.gov/Archives/edgar/data/1018724/000119312512155627/filename1.htm.

Securities and Exchange Commission (SEC). (2018). Commission Statement and Guidance on Public company Cybersecurity Disclosures. Retrieved from https://www.sec.gov/rules/interp/2018/33-10459.pdf.

Securities and Exchange Commission (SEC) (2018a). EX-99.1 2 d577037dex991.htm EX-99.1. Retrieved from https://www.sec.gov/Archives/edgar/data/1011006/000119312518131302/d577037dex991.htm

Sherman, N. (2015, August 14). After cyberattack, CareFirst faces class action suit. *The Baltimore Sun*. Retrieved from https://www.baltimoresun.com/business/bs-bz-carefirst-suit-20150814-story.html.

Wang, T., Kannan, K. & Ulmer, J. (2013). The association between the disclosure and realization of information system risk factors. *Information Systems Research,* 24 (2), 201-218.

White, M. (2013, May). "Letter from White to Senator Rockefeller Regarding Cyber Security Disclosure." Retrieved from https://www.commerce.senate.gov/public/_cache/files/7b54b6d0-e9a1-44e9-8545-ea3f90a40edf/707DAF7FB7719BCE1FAF921109FAE148.512013-letter-from-sec-chair-white.pdf.

Yahoo (2013, 2014, 2015, 2016) Form 10-K Annual report. Retrieved from http://www.annualreports.com/Company/yahoo.

Young, S. (2013). Contemplating Corporate Disclosure Obligations Arising from Cybersecurity Breaches. *The Journal of Corporation Law*, 38-3, 660-679).