UCONN LIBRARY

University of Connecticut
OpenCommons@UConn

Honors Scholar Theses | Honors Scholar Program

Spring 5-1-2022

SEC Reporting of Cybersecurity Incidents

Michaela Morosky
michaela.morosky@uconn.edu

Follow this and additional works at: https://opencommons.uconn.edu/srhonors_theses

 Part of the Accounting Commons

Recommended Citation

Morosky, Michaela, "SEC Reporting of Cybersecurity Incidents" (2022). *Honors Scholar Theses*. 870.
https://opencommons.uconn.edu/srhonors_theses/870

SEC Reporting of Cybersecurity Incidents

Michaela Morosky

University of Connecticut School of Business
Department of Accounting
Undergraduate Honors Thesis

Thesis Supervisor: Alina Lerman
Honors Advisor: Alina Lerman

May 2022

1. Introduction

All organizations have become increasingly reliant on technology to conduct their operations over the past several decades. Both businesses and government entities use complex information technology systems and collect vast amounts of sensitive data. This newfound reliance on technology has created complex security threats for businesses and their stakeholders, such as customers and suppliers. The growing dependence on these technologies and the existence of vulnerabilities in them is resulting in increased frequency and severity of cybersecurity attacks (Rosati, Gogolin, and Lynn 2020).

According to the National Initiative for Cybersecurity Carriers and Studies [NICCS], a cybersecurity attack is "an attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity." Attacks can be active where the perpetrators attempt to alter some system or data or passive where they obtain unauthorized information. Cybersecurity incidents can also include unintentional events such as data losses. All types of cybersecurity incidents can have disastrous effects on their victims. Perpetrators can disrupt normal business operations by accessing critical systems, corrupting company data, and gaining unauthorized access to protected sensitive data.

Cyber attacks have financial mitigation costs as well as reputational costs for the target company and economy-wide costs and implications. According to Smith and Lostri (2020), it is estimated that cybercrime has resulted in a staggering 1 trillion-dollar yearly strain on our economy since 2018. In 2020, the annual monetary loss directly from cybercrime was estimated to be 945 billion dollars, with global spending in response exceeding 145 billion dollars. These numbers represent a 50% increase in spending since 2018 and 1% of global gross domestic product. While some of the increase may be attributed to better reporting, the bulk is likely

driven by crime growth. In a survey conducted by Smith and Lostri (2020), among 1,332 respondents who fell victim to a cyber incident in 2019, 45% invested in new cybersecurity software, 39% increased the company budget for cybersecurity incidents, and 30% hired new IT security staff. It is not surprising that an increase in security spending often follows the company's discovery and reporting of a vulnerability. With a growing reliance on cyberspace to conduct operations, the costs to combat and prevent vulnerabilities are also on the rise.

The Sarbanes-Oxley Act of 2002 [SOX] put in place several initiatives to promote the stability of the national financial system and improve the reliability of financial information systems. Section 404 of SOX requires all publicly traded companies to establish effective internal controls and procedures to safeguard financial reporting. It also requires that the annual reports of these firms include both the firm's and the independent auditor's assessment and attestation of these internal controls. One of the main goals of these controls is to ensure the integrity of financial data. Reports of material weaknesses from either the management or the auditor indicate weak internal controls. SOX creators did not explicitly have cybersecurity in mind and rather were focused on preventing unethical manipulation of financial reporting by management and other company insiders. However, as the digital era has reshaped data security since 2002, it is easy to see that efficient internal controls may also aid with cybersecurity risks. Correspondingly, reported material weakness of internal controls may be silent indicators of a higher risk of cyber breaches and their costs.

Investing in internal controls and, more generally, information security is a growing necessity for all firms and can minimize the likelihood and severity of cyber incidents. Gordon and Loeb (2002) recognized the priority of increased spending to combat cyber threats and created the Gordon-Loeb model to determine the optimal amount organizations should invest in

information security. Hausken (2006) highlights investments in security technology are in the organization's best interest when the expected rate of return on the investment exceeds the average cost of a cyber attack. Even with these preventive measures in place to minimize the likelihood of a cybersecurity attack, an incident may still occur. Therefore, firms must have consistent policies and procedures for informing the relevant stakeholders, including investors, that a cybersecurity breach occurred.

At this time, there are no rules or laws associated with cybersecurity disclosures. The Securities and Exchange Commission [SEC] has released some guidance on best practices when assessing a cybersecurity incident. The SEC's first guidance was released in 2011 to help firms make disclosures that fit the standards of the Securities Act of 1933 and the Securities Exchange Act of 1934. Several years later, in 2018, the SEC released its second guidance, which sought to reinforce and expand 2011's staff guidance by providing additional information when making disclosures regarding cybersecurity incidents and risk factors. Importantly, both guidance editions provide only a loose framework of suggestions and do not normalize the format, timing, or substance of disclosures for any cybersecurity incidents.

The lack of standardization within the cybersecurity risk disclosure is increasingly becoming a cause of concern among regulatory officials. On March 9, 2022, the SEC published Release 33-11038, a proposal for new "rules and amendments to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and indecent reporting by public companies." If the SEC can generate enough support to finalize this new rule, the updated cybersecurity disclosure regulation will provide investors and other information users with more timely information relating to cybersecurity risks and incidents. The supporters of the proposal argue that this would enable stakeholders to better mitigate those respective risks

and incidents. The two areas discussed within this proposal include specific incident disclosure and, more general, risk management, strategy, and governance disclosures.

The proposed incident disclosure places a judgement of materiality front and center – the proposed rule has 118 references to the word "material." This raises a complex question of what constitutes materiality. Several law cases such as *TSC Industries, Inc v. Northway, Inc, Basic, Inc v. Levison and Matrixx Inciatives, Inc. v. Siracusano* has provided valuable insight into this issue. A public organization experiences a material breach when the compromised information has a substantial likelihood to be important to a reasonable shareholder, to current or potential investment decisions, and/or results in any significant alteration to the 'total mix' of information that is made available to shareholders. Previously, cyber disclosures proposed by the SEC's 2011 and 2018 guidance recommended that it was best practice of an organization to include cybersecurity incidents in disclosure when the breach was determined to be material in nature. However, it neither mandated this nor provided a suggested disclosure format. SEC Release 33-11038 aims to modify the list of events requiring a Form 8-K filing to include cybersecurity incidents. This would require the registrants to disclose such events within four business days upon the discovery of a material cybersecurity incident. This requirement would ensure timely reporting of breaches upon discovery and consistency between public firms.

SEC Release 33-11038 also includes proposed updates to the risk management, strategy, and governance disclosure. Rather than the actual incidents, this area regards enhancements of preventative measures firms take to prepare themselves against the risk of potential breaches. This new requirement adds regulation 106 to form S-K to "describe its policy and procedures, if any, for the identification and management of risks from cybersecurity threats, including whether the registrant considers cybersecurity as part of its business strategy, financial planning and

capital allocation." The guidance would apply even to foreign private issuers. It proposes to add Item 16J of form 20F to require annual reporting of cybersecurity policies, procedures and strategies. SEC's implementation of these new cybersecurity requirements is directed to strengthen overall internal controls with the goal of creating consistency amongst breach reporting and cybersecurity disclosures.

This paper documents the reporting to the SEC of 197 major incidents of cybersecurity breaches among public firms in the years 2011-2019. My goal is to contribute to the debate on the need to revise the disclosure guidance by evaluating the extent to which cybersecurity breaches are disclosed in SEC filings under the current regulatory regime. In evaluating the individual breaches, I document whether prior to the SEC's 2022 proposed amendment, firms were already following the SEC recommendation of disclosing material cybersecurity breaches in a timely manner. I find that it is extremely rare for a firm to follow the recommendations set by the SEC. The majority of companies that experience a cybersecurity breach did not make formal disclosure in SEC filings even when a substantial number of customer files were affected in the breach. This study also shows that among the firms that did disclose the breach to the SEC, most did not follow the SEC's proposed four-day timeline and only provided very minimal information in the actual disclosure.

My findings suggest a significant inconsistency and suboptimality in existing disclosure practices. Given the growing number of annual cybersecurity incidents and the continued expected growth in reliance on technology, the results lend support to the SEC's current proposals to formalize timely and substantive disclosures of these issues.

2. Background

2.1 Prior Literature

Research conducted by Amir, Levi, and Livne (2018) is closely related to the objectives of this paper. According to their study, when a breach is classified as a material cyber attack, pertinent information should always be disclosed to inform all necessary parties. However, firms often are found underreporting instances of cyber attacks, likely as a direct result of incentives held by management to withhold negative information and the belief that investors are unlikely to discover a cyber attack independently. To evaluate the degree public companies are withholding reports of cybersecurity incidents, the authors analyze data of cyber attacks from 2010 to 2015, discovering that only 300 public firms made disclosures related to cyber incidents while independent sources reported over 1,000. Their findings suggest that managers disclose cyber attacks only when investors already suspect that, with a 40% chance, an attack has occurred. The authors conclude that voluntary disclosure of cyber attacks is rare. I build on this work by focusing on a more recent sample when the market participants are more aware of cybersecurity threats and expect greater disclosure and by examining the method and details of the disclosure itself.

Cybersecurity incidents have also increased audit risk awareness when conducting audit reports of affected firms. Rosati, Gogolin, and Lynn (2020) assess the implications of cybersecurity incidents for audit quality on a sample of 329 incidents from Privacy Rights Clearinghouse from 2005 to 2014. They focus on audits carried out by the Big Four audit firms to ensure consistency among auditors and clients. The authors conclude that cybersecurity incidents do not result in an observable deterioration in audit quality. Rather the opposite

conclusion is made, showing that auditors of breached firms increase substantive testing and audit efforts, and this higher scrutiny leads to an observed increase in audit quality.

Information asymmetry between organizations and investors is another factor influencing cybersecurity risk disclosure among public companies. Research conducted by Cheong, Yoon, Cho, and No (2021) explores how the growth of cybersecurity breaches puts stakeholders' welfare at risk. This study examines the informativeness of the firm's cybersecurity risk disclosure, highlighting them as the primary source of data for stakeholders seeking to gauge the cybersecurity risks of the firms. The authors analyze 25,179 cybersecurity risk disclosures from 2006 to 2017. The analysis suggests that firms do not provide a sufficient amount of disclosure after experiencing a cybersecurity breach. Firms provide more information about the risks derived from a third party and less disclosure about their own incident control and risk mitigation, and business continuity. Often firms provide information that does not support the overall informativeness of disclosure, such as focusing on control-related damage mitigation factors rather than the relevant vulnerability-related factors. Inconsistencies in presentation among firms create a universal disclosure obfuscation, reducing the informativeness gained from disclosures.

A practitioner work "The Hidden Costs of Cybercrime" by Smith and Lostri (2020) recognizes the substantial costs of cybersecurity breaches. Analysis of 1,500 company surveys showed that only 4% did not have a cyber incident in 2019. Furthermore, 92% of those who did experience an incident recognize the damages that span beyond just the financial costs. Highlighting the persistence of the problem, results showed that more than 50% of those interviewed did not have plans to prevent cybersecurity incidents, and of those who did, only 32% believed their plans to be effective. Hidden costs often associated with cybercrime include

opportunity costs, system downtime, reduced efficiency, brand damage and loss of trust, incident response costs, and cyber risk insurance.

The preceding literature covers some of the pressing issues already researched and discoveries made in relation to cybersecurity disclosures. This paper will build on and contribute to this literature by using the reporting data to infer the firms' formal disclosure procedures and processes when impacted by a breach.

2.2 Institutional Detail

As of the writing of this paper in the spring of 2022, there is no official guidance issued by the SEC with regard to cyber incident disclosure. Thus, important questions open to interpretation are: what constitutes a security breach, when is it necessary to disclose, and what are the proper disclosure procedures. Any cybersecurity disclosure made at this time is voluntary and up to the firm's discretion in terms of timeliness and content. There are likely limited legal repercussions to insufficient disclosure of a cybersecurity incident, however, the firm could face reputational damages from customers and investors. To provide insights into recommended procedures, the SEC has issued two pieces of guidance addressing the growing topic of cybersecurity over the past decade.

Its first guidance issued in 2011 acknowledged the growing reliance on technology to conduct business operations while also recognizing the risks associated with its newfound dependence. To better inform investors regarding potential risks, it suggested that it is the responsibility of the organization to provide disclosure of the inherent risk factors that may influence stakeholders' perception of the riskiness of the firm. To maintain the SEC's fundamentals of timely, comprehensive and accurate information it put forth the expectation that organizations properly disclose instances of cybersecurity risk or incidents determined to be

material in nature. The SEC's 2011 guidance identifies an event or information as *material* if it would cause a reasonable investor to reevaluate investment decisions or alter company perception.

The second regulatory update was released in 2018 as a means for the SEC to provide further guidance in light of the growing instances of cybersecurity incidents. It included two topics not included in the 2011 edition issued by the SEC, the importance of cybersecurity policies and procedures and insider trading prohibition in cybersecurity. In the guidance, the SEC recommended that all organizations establish efficient disclosure controls and procedures to ensure that any relevant information about the cybersecurity incident is made known to the appropriate personnel. They also specified that procedures should be put in place to prevent directors, officers, or company insiders from making trades based on material nonpublic information regarding cybersecurity risks and incidents facing the company. Preventing any company officials from an unfair advantage due to insider information that has not been made public with respect to cybersecurity is aligned with other anti-fraud laws. Incorporating these new provisions and elaborations of prior recommendations allowed for further insight into how organizations should address cyber threats.

A concern about mandating detailed disclosure on cybersecurity threats and defenses is that following these recommendations could create a "roadmap" for those seeking to penetrate a company. In other words, providing so much detail into what occurred within the organizations and the preventative measures could be seen as providing cybercriminals instructions on how to successfully breach that or other organizations in the future. The SEC commented on these concerns stating that they do not expect nor recommend organizations provide such detail regarding specific, technical information about cybersecurity systems or any potential

vulnerabilities that would inherently make the organization more susceptible to a cybersecurity incident. Rather it is advised that all firms take the necessary steps to inform the public of material breaches that would likely influence investors' decisions in relation to the firm.

All information pertaining to cybersecurity disclosures should provide accurate, timely, and comprehensive information when a breach has occurred. The organization itself should not be the only focal point when making a cybersecurity disclosure. It should also make an effort to give investors the chance to make an educated decision regarding their investment. To accomplish this feat, organizations should be making disclosures when the impact of the attack is determined to be material in nature. When this type of breach occurs, the organization should adequately describe the intellectual property stolen and note if the reported financial information is compromised or is no longer an accurate representation of future operating results or company financial condition.

2.3 Hypotheses

Given that the SEC has no formal rules and regulations regarding cybersecurity disclosure and promotes voluntary disclosure, it is no surprise that the lack of legal consequences for failing to disclose a breach has resulted in firms creating their own disclosure procedures leading to inconsistency between firms. This paper aims to highlight procedures in which public organizations disclose instances of cybersecurity events, if at all. In doing this, the first part of my paper will be descriptive. Focusing on a sample of large breaches, I will document how they are reported to the SEC. While firms may disclose breaches in other forms (press releases, on their website), it is critical to recognize that SEC EDGAR system is the centralized, public repository of information. Thus, it is important to understand how these incidents are reported to their system.

Upon analyzing the research conducted by prior literature, I believe that organizations will be more likely to make a formal 8-K cybersecurity disclosure if a larger number of records become compromised in a breach. I propose that any organization that experiences a cyber incident that compromises more than approximately a million client records, whether that may be usernames and passwords or private personal information, will issue a corresponding 8-K. In instances where less than a million client records were compromised, I expect the incident will not be formally disclosed in the 8-K, but rather will only be addressed in a press release or in secondary sources.

I will examine whether firms which have reported material internal control weaknesses are more likely to disclose the cybersecurity incident. I do not offer a prediction on the direction of this relationship. On the one hand, firms that have material weaknesses may have a poorer information system overall, and thus the management may not have the sufficient information to file a Form 8-K. On the other hand, these firms may be actively mitigating this weakness, and the extra scrutiny from internal and external auditors or other stakeholders may lead to more reporting.

I will also provide further descriptives on the timeliness and extent of SEC disclosures. Due to the likely absence of legal consequences from regulatory bodies when failing to make voluntary disclosures, I expect a large variance and overall relatively poor quality. I believe that if a firm decides to report its breach, there is a high likelihood that it will not meet the SEC's recommendation of disclosure within four business days upon discovery**.**

3. Data and Methodology

The dataset of cybersecurity breaches used to test these theories was retrieved from Privacy Rights Clearinghouse (PRC) website. Established in 1992, PRC is a nonprofit

organization whose mission is focused on helping people find answers to complex questions by publishing informative materials with the overall objective of protecting privacy for all. The dataset is a comprehensive list of known data breaches starting in 2005. The data includes key information such as organization name, location, a description of the breach, company industry, a type of breach, and the year it occurred.

Upon initial collection, the PRC dataset consisted of 9016 entries of data breaches ranging from 2004 to 2019. To obtain the final dataset, I made several decisions to reduce the sample size to identify the most relevant sample for manual analysis. See Table 1 for the full sample selection. First, I reduced the dataset to focus only on companies included in the S&P 500 as of 2021, which resulted in 360 entries. This was done to ensure all breaches were for public companies that follow SEC reporting standards and to focus on large firms more likely to be both targeted by material threats and concerned about reputational costs. Then I decided to eliminate all entries occurring before 2011, to reflect the complete lack of guidance for cybersecurity disclosure procedures until 2011. Next, I eliminated cybersecurity incidents that entailed more than one entity to focus only on firm-specific incidents. This reduced the dataset to 197 entries.

For each of the 197 security incidents, I carried out a manual analysis of SEC filings of 8-K and 10-K forms to identify the primary method of disclosure to the SEC. An 8-K report is a 'current report' that firms use to disclose to the SEC and the stakeholders major events in a timely manner. While there are a number of specific items which must be disclosed in an 8-K (such as a bankruptcy, an impairment of assets, a change of management, etc.), importantly, the guidance states that other non-specified events must also be disclosed under the item of "other events" if they are material. Thus, if the firms deem a security incident material, they should

disclose it within four business days as encouraged by the SEC from 2011 and as the currently proposed guidance seeks to mandate. After collecting the date of the incident recording in the PRC dataset, I examine the 8-Ks filed from 6 months before to 6 months after the incident. I focus on 8-Ks filed with an item 8.01 "other events" disclosure referring to the cyber incident.

I also examine the 10-Ks of these firms to identify whether they are disclosing these incidents in periodic filings. This allows me to examine how firms are trading off timely reporting of an event when information may yet be incomplete or a delayed reporting of a more thorough and complete nature. Form 10-K, otherwise known as the 'annual report,' provides a comprehensive overview of the company's business and financial condition and includes audited financial statements. As such, even if no timely disclosure of an event happened in an 8-K, it is reasonable to expect that some disclosure in the annual report is appropriate to give stakeholders a full picture of the cyber landscape of the firm. I examine the first 10-K filed following the date of the incident. Table 2 contains a list of terms I use to conduct a keyword search for cyber breach disclosure.

4. Findings

4.1 Frequency and Timeliness of SEC Reporting

I start by summarizing how many data breaches receive any disclosure in the SEC filings. Figure 1 presents the dramatic lack of SEC reporting of cyber incidents among the examined firms. Out of a sample of 197 security breaches, only 19 firms made the relevant disclosures to the SEC (all these firms and incidents are listed in Appendix A). Figure 2 illustrates the actual format of disclosure. My original expectation was to observe a somewhat timely 8-K disclosure in line with the 2011 and 2018 SEC recommendations, although likely not following the currently proposed four-day reporting guidance. Contrary to my expectations, I found that out of

the reporting sample, only 42 percent reported the incident in an 8-K. In contrast 58 percent (of the already small reporting sample) discussed the cyber issue in a much less timely periodic 10-K report. Notably, every firm that reported the incident in an 8-K, followed up with a 10-K disclosure that reiterates or elaborates the discussion of the incident. I further examine the speed of the 8-K reporting in Table 3. I observe that even for the 8 firms that reported the incident in these 'current reports,' they didn't do it in a timely manner. The mean and median number of days between the incident (per PRC database) and the 8-K filing date is 22 and 16 days, respectively, while the max is over two months (Figure 3). Only 1 firm, Under Armor, met the four-days requirement put forth in the current guidance proposal.

I hypothesized that larger incidents are more likely to generate timely disclosure. Specifically, I predicted that breaches compromising greater than one million customer files constitute a material cybersecurity incident requiring disclosure. The data supports my expectations. Table 4 shows the number of customers impacted for the incidents reported via an 8-K, a 10-K only, or not at all. I first note the pattern of means and medians consistent with my expectations. The mean customer files affected for firms with the most timely reporting via an 8-K is 109 million. When firms chose to disclose only in the annual 10-K filing, the average customer files number affected was substantially smaller at 17.5 million. This suggests that for moderate breaches that the organization believes warrant a disclosure, they will likely opt to only disclose in the 10-K. Lastly, the mean number of customer files affected for firms that chose not to disclose in any manner is very small at 0.25 million. This supports my initial assumption that when customer files fall below 1 million, firms will likely choose not to disclose cybersecurity instances to the public. The medians show a similar trend across the three groups.

It is interesting to also consider the minimum and maximum values. It is possible that a cybersecurity incident impacts zero customers, if the underlying data is not customer-related. However, all eight of the 8-K disclosures are customer-related in contrast to the other two groups. Contrary to my expectations, the maximums illustrate that even when millions of customers are impacted, the firms may omit disclosures or make only non-timely ones. Despite this surprising note, my overall conclusion is that the number of customer files affected positively influences both overall disclosure probability and disclosure timeliness.

4.2 Length and Nature of Reporting

Next, I quantify the amount of detail provided in the actual disclosures included in the 8-K and 10-K reports. Table 5 illustrates the length of the disclosure provided by the organization to address the cybersecurity incident. Given the increased timeliness of an 8-K disclosure with desired disclosure falling within a 4-day timeline it is no surprise to see the 8-K results of lengths of disclosure were very brief, in many cases providing a quick overview of what was found. The results in Table 5 illustrate that the mean and median length of the relevant 8-K reporting in sentences were 5 and 2, respectively. The most detailed 8-K contained only 14 sentences and the briefest one a mere 1 sentence. The 10-K disclosure provided a slightly different story, which likely is attributed to the increased time the organization had to evaluate what went wrong and the full effect of the cybersecurity breach. When evaluating the annual 10-K reports of the 19 organizations that made a cybersecurity disclosure, the mean and median were 15 and 13 sentences, respectively, with a maximum of 33 and a minimum of 7.

The results presented in Table 5 shed light on how much detail is provided when firms make a cybersecurity disclosure. I found the very limited extent of disclosures in the 8-K reports quite surprising. Even amongst the firms that attempt to meet the SEC cybersecurity

recommendations for making an informative disclosure, a bare minimum of information is contained within the report alone. Generally, most reports just state that the organization had a cybersecurity breach and, in some cases, mention the cause, such as a hack or other means of infiltration. In the 10-K reports, the informativeness was higher in comparison to the 8-Ks, but overall even there, it did not meet my expectation of the depth of information that would be relevant to investors. These findings support the argument that the SEC should make formal requirements as to what should be included in both length and content to make adequate representation to investors and to ensure consistency among all firms.

4.3 Internal Control Weaknesses and Incident Reporting

As previously stated, I believe that material weaknesses associated with an organization's internal controls could be associated with less disclosure if they indicate a lack of appropriate internal information systems. On the other hand, they could be associated with more disclosure due to higher scrutiny. Table 6 tabulates all firms that filed a report indicating an internal control material weakness among my original dataset of 197 company breaches. I report how these firms disclosed their breaches. Out of the 11 firms that reported an internal control deficiency, two firms (Marriott International and eBay) made SEC disclosure. Thus the reporting percentage of firms with internal control issues (2/11 = 18%) is higher than the reporting percentage of firms without internal control issues (17/186 = 9%). I found it interesting that these 2 organizations filed internal weakness reports after their cybersecurity breaches (1 year later for Marriott International and 2 years later for eBay). This surprised me because I would expect that the cybersecurity breach would be a strong indicator that an organization may have weak internal controls, given that someone was able to infiltrate their system. Why did it take so long for each

organization to file a report to identify that they suffer from compromised or weak internal controls? Or why did they not remedy this situation sooner?

5. Conclusions

A growing dependence on technology to conduct everyday operations increases the damage sophisticated cybercriminals can inflict on firms. When it comes to infiltration of an organization's private security, perhaps it is not a matter of *if* but rather *when*. Therefore, it is in the best interest of all organizations to manage risk and properly disclose issues to minimize reputational damage in the eyes of investors and customers. This paper examines 197 cybersecurity breaches of S&P 500 companies that occurred after the first SEC suggested disclosure guidance in 2011. I find that only 10% of the sample reported cyber incidents in the 8-K or the 10-K. Among this small sample, only 42% reported the issue in both current and annual reports, and 58% reported solely in the less timely annual report. Among the firms that did provide an 8-K disclosure, shockingly, only 1 firm followed the SEC's four-day recommendation. I find that firms gave little detail into the actual breach, providing, on average, only 5 sentences in the 8-K disclosure and 15 sentences when filing a 10-K. I found that the number of customers affected by the breach appears to be positively associated with disclosure likelihood. Surprisingly, I did not observe any association between breach reporting and internal control weaknesses.

Overall, these results provide further support for the need to normalize policies and procedures regarding cybersecurity disclosure to maintain consistency among all firms in this evolving topic. I believe the new SEC Release 33-11038 takes a step in the correct direction by proposing guidance on the content and timeliness of cybersecurity-related disclosures.

References

About. Privacy Rights Clearinghouse. (n.d.). Retrieved March 22, 2022, from https://privacyrights.org/about

Amir, E., Levi, S. & Livne, T. Do firms underreport information on cyber-attacks? Evidence from capital markets. Rev Account Stud 23, 1177–1206 (2018). https://doi.org/10.1007/s11142-018-9452-4

Cheong, A., Yoon, K., Cho, S. & No, W. Classifying the Contents of Cybersecurity Risk Disclosure through Textual Analysis and Factor Analysis (2021). *Journal of Information Systems* (2021) 35 (2): 179–194. **https://doi.org/10.2308/ISYS-2020-031**

Conformed to federal register version - SEC. (n.d.). Retrieved January 17, 2022, from https://www.sec.gov/rules/interp/2018/33-10459.pdf

Cybersecurity glossary. National Initiative for Cybersecurity Careers and Studies. (n.d.). Retrieved January 17, 2022, from https://niccs.us-cert.gov/glossary#I.

Cybersecurity. (2011, October 13). Retrieved January 17, 2022, from https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

Cybersecurity. (2018, February 26). Retrieved January 17, 2022 from https://www.sec.gov/rules/interp/2018/33-10459.pdf

Data breaches. Privacy Rights Clearinghouse. (n.d.). Retrieved March 22, 2022, from https://privacyrights.org/data-breaches

Fast answers. SEC Emblem. (2012, August 10). Retrieved March 22, 2022, from https://www.sec.gov/fast-answers/answersform8khtm.html

Pierangelo Rosati, Fabian Gogolin & Theo Lynn (2020) Cyber-Security Incidents and Audit Quality, European Accounting Review, DOI: 10.1080/09638180.2020.1856162

The hidden costs of cybercrime. Home - (ISC)Â² Community. (2020, December 21). Retrieved April 22, 2022, from https://community.isc2.org/t5/Industry-News/The-hidden-costs-of-cybercrime/td-p/41628

Table 1: Sample Selection

	Number of Entries
Cases Listed in Privacy Rights Clearinghouse's Data breach Chronology	9,016
Less: Companies not included in S&P 500	(8,656)
Less: Breaches before 2011	(104)
Less: Joint company breaches	(59)
Final Sample	**197**

Table 2: Keywords searched in 8-K/10-K filings

Cyber Breach Incident Security Data breach Infiltrated Unauthorized Attack	*Keywords used to search for references of cyber incidents in 8-K/10-K to categorize occurrences as reported vs. not reported.

Table 3: 8-K Timeliness

Variable	N	Mean	Median	Min	Max	Standard Deviation
Days between Breach Discovery Date and 8-K Filing Date	8	22.35	16	4	70	22.47

Table 4: Reporting Type and Incident Impact

Variable	N	Mean	Median	Min	Max	Standard Deviation
Customers Affected (in millions) – Firms which made initial 8-K Disclosures	8	109	101	1	327	108
Customers Affected (in millions) – Firms which made initial 10-K Disclosures	11	17.5	.4	0	78.8	30.7
Customers Affected (in millions) – Firms which did NOT make Disclosures	178	.25	.0017	0	32	2.4

Table 5: Reporting Length

Variable	N	Mean	Median	Max	Min	Standard Deviation
Length 8-K Disclosure (sentences)	8	5.25	2	14	1	5.04
Length 10-K Disclosure (sentences)	19	14.67	12.5	33	7	7.023

Table 6: Reported Internal Control Weaknesses

Company Name	CIK	FYE of IC Weakness	Cybersecurity Incident Reported?
Baxter Healthcare	10456	12/31/19	No
Stanley Black & Decker Inc.	93556	1/2/21	No
Lockheed Martain	936468	12/31/16	No
Iron Mountain	1020569	12/31/11	No
Marriot International	1048286	12/31/19	Yes (2018)
Crown Castle International Corp	1051470	12/31/19	No
eBay	1065088	12/31/16	Yes (2014)
MetLife	1099219	12/31/17	No
DXC Technology	1658688	3/31/20	

Figure 1: Reported vs. Not Reported Incidents

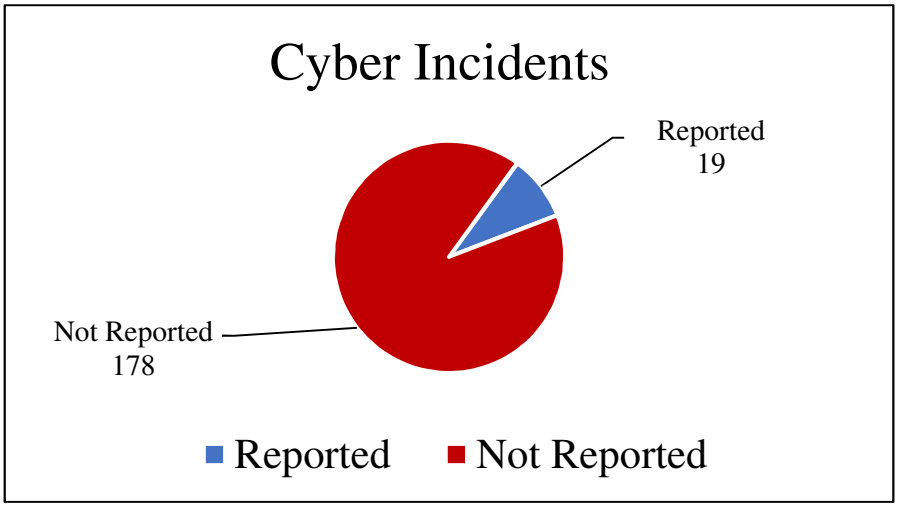


Figure 2: 8-K vs. 10-K Reporting (sample of 19)

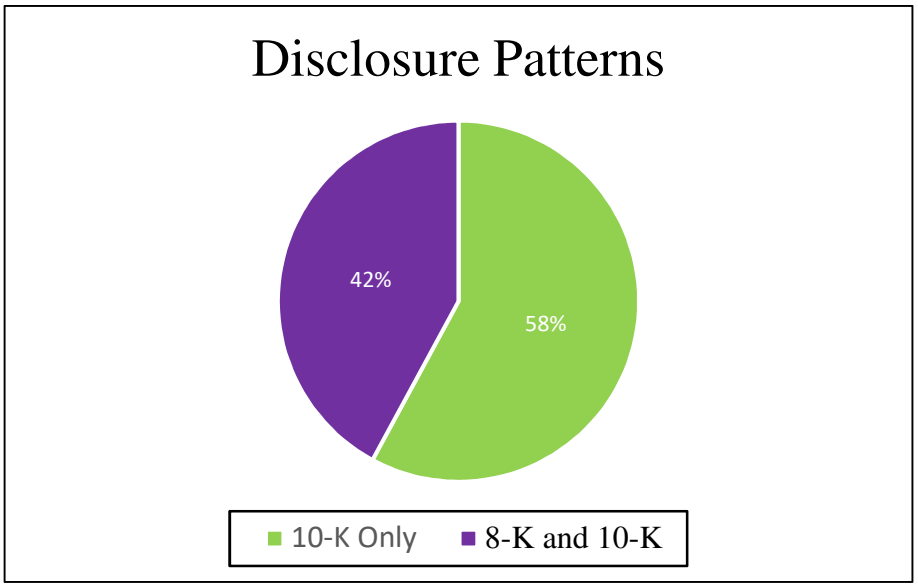
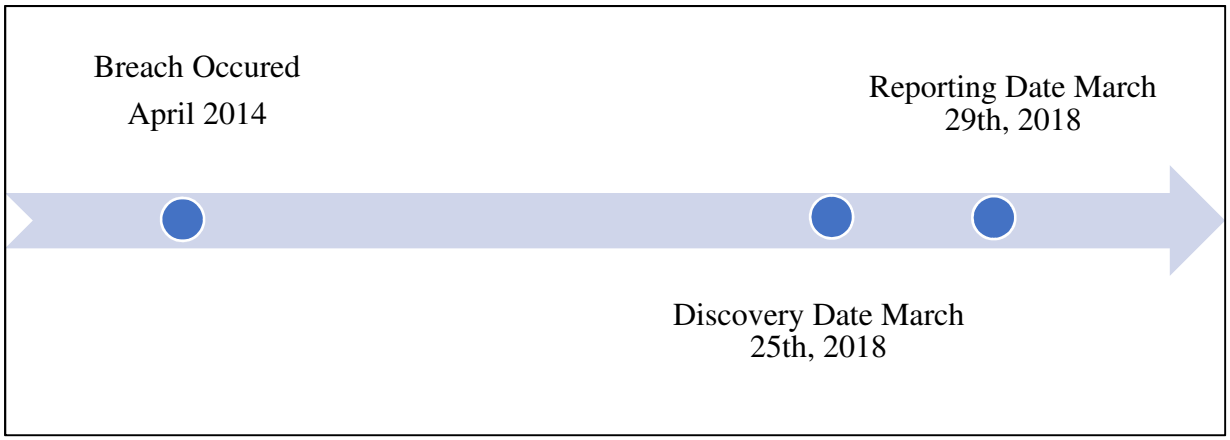
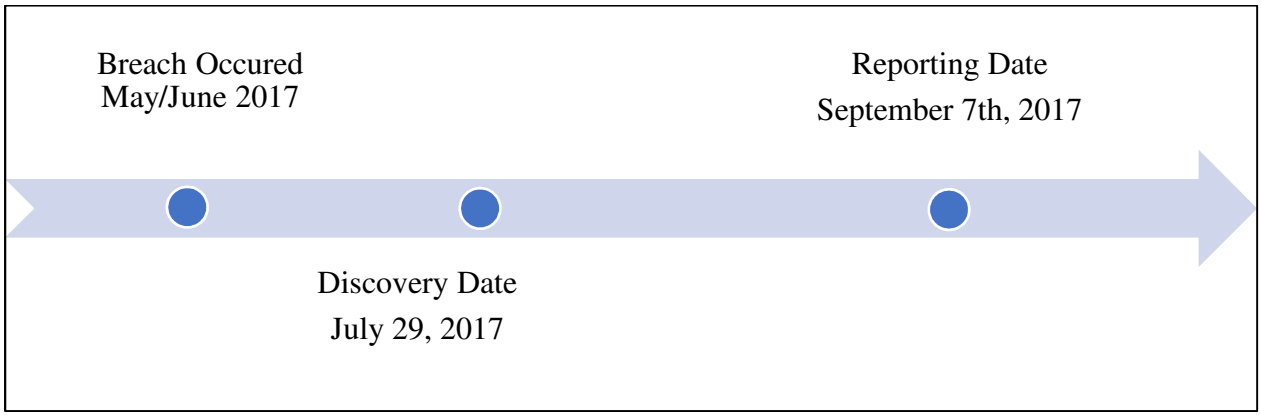


Figure 3: Timeline of Two Company Disclosures

Fastest: Under Armor (2018)
Customers Affected: 150 million



Slowest: Equifax Corporation (2017)
Customers Affected: 145 million



Appendix A: Reported Cybersecurity Breaches

Company	Discovery Date	Customers Effected	8-K Disclosure Date	Length of Disclosure	Exhibits	10-K Disclosure Date	Length
Marriot International	11/19/2018	327,000,000	11/30/2018	2 Pages	Press Release	12/31/2019	1.5 Pages
Google	10/8/2018	500,000	N/A	N/A	Press Release	12/31/2018	2 Paragraphs
T-Mobile	8/24/18	74,000,000	N/A	N/A	Press Release	12/31/2018	5 Sentences
Under Armor	3/25/2018	150,000,000	3/29/2018	2 Sentences	Press Release	12/31/2018	1 Paragraph
FedEx	2/19/2018	119,000	N/A	N/A		5/31/2018	1 Paragraph
Equifax Corporation	7/29/2017	145,500,000	9/7/17	2 Sentences	Press Release	12/31/2017	2 Pages
Verizon	6/13/17	6,000,000	N/A	N/A	Press Release	12/31/2017	2 Paragraphs
Chipotle Mexican Grill	4/25/17	0	N/A	N/A	Press Release	12/31/17	2 Paragraphs
Quest Diagnostics	11/26/16	34,055	N/A	N/A	Press Release	12/31/2016	3 Paragraphs
Twitter	6/13/16	32,000,000	N/A	N/A		12/31/2016	1 Paragraph
Centene	Not Disclosed	950,000	1/25/2016	2 Sentences	Press Release	12/31/16	1 Paragraph
Anthem Inc	1/29/15	78,800,000	N/A	N/A	Press Release	12/31/2015	4 Paragraphs
Home Depot	9/2/14	56,000,000	9/8/14 9/18/14	1 Page/3 Pages	Press Release	2/1/15	5 Pages
eBay	Early May 2014	145,000,000	5/22/14	1 Sentence	Press Release	12/31/2014	2 Paragraphs
Target	12/13/13	40,000,000	2/26/14	3 Pages	Press Release	2/1/14	3 Pages
NASDAQ.com	7/18/13	0	N/A	N/A	Press Release	12/31/13	2 Paragraphs
Citigroup	7/17/13	146,000	N/A	N/A	Press Release	12/31/13	3 Pages
Nvidia	7/13/12	400,000	N/A	N/A	Press Release	1/23/13	1 Paragraph
Global Payment Inc	Not Disclosed	7,000,000	3/30/12	2 Sentences	Press Release	5/31/13	4 Paragraphs