Journal of Forensic and Investigative Accounting
Volume 12: Issue 2, July–December 2020

The Impact of Cyber Breaches on the Content of Cybersecurity Disclosures

Orry Swift
Ricardo Colon
*Kelly Davis**

I. Introduction

Since the 1980s, the criminal or unauthorized use of electronic information has been prevalent in many public sector corporations. To protect from this threat, firms adopt practices to protect the confidentiality, integrity, and availability of data and assets in cyber space (Schatz et al., 2017). The literature refers to these measures and practices as "cybersecurity." Firms can devote all their resources to cybersecurity and not be totally "secure", which makes cybersecurity a material business risk (Tuma and Rucker, 2018). Like other business risks, management has an obligation to disclose material risks related to cybersecurity.

With respect to cybersecurity disclosures, the U.S. Securities and Exchange Commission (SEC) has issued two sets of guidance. The first guidance, titled *CF Disclosure Guidance: Topic No. 2 - Cybersecurity,* called firms to disclose: (1) aspects of the business or operations that give rise to material cybersecurity risks and the potential costs and consequences; (2) outsourced functions that have material cybersecurity risks and information on how the firm addresses those risks; (3) the occurrence of cyber incidents that are individually, or in aggregate, material, including information about costs and consequences; (4) risks related to cyber incidents that may remain undetected for an extended period; and (5) information regarding cyber security insurance coverage (SEC, 2011). The second guidance, an interpretive release issued in 2018, calls public companies to "take all required actions to inform investors about material cybersecurity risks and incidents in a timely fashion, including those companies that are subject to material cybersecurity risks but may not yet have been the target of a cyber-attack" (SEC, 2018).

Similarly, the American Institute of Certified Public Accountants has unveiled a "Cybersecurity Risk Security Management Reporting Framework" which may be used to by management to inform and describe its cybersecurity risk management program and used by CPAs to report on management's description (AICPA, 2017). More importantly, under Section 302 of the Sarbanes-Oxley Act, the principal executive officer of a firm is required to certify the information contained in the issuer's quarterly and annual reports certifications is true and correct, including disclosures regarding internal controls for identifying cybersecurity risks and incidents and for assessing their impact on the financial statements.

There is a dearth of research in the academic literature regarding cybersecurity disclosures and, more specifically, the impact of cyber breaches on cybersecurity disclosures. The lack of research on this topic is particularly troubling given the consistent increase in the number of cybersecurity incidents reported by public companies and concerns that current cybersecurity disclosures are inadequate because they contain mostly boilerplate language (Ferraro, 2014). This study seeks to fill the void in the academic literature by using text-based analysis of the Management Discussion and Analysis (MD&A) section of annual reports to determine how the occurrence of a cyber breach impacts the content of cybersecurity disclosures analyzing the following textual characteristics: length, boilerplate, fog, specificity, and tone

This study makes a twofold contribution to existing literature. First, to the author's knowledge, it is the first study to employ various textual analysis techniques used in prior accounting studies to analyze the impact of a cyber security breach on the content of financial statement disclosures. Second, our study finds a significant relationship between the occurrence of a cybersecurity breach and certain attributes of cybersecurity disclosures of importance to investors. With respect to the use of boilerplate language, which has been the focus of criticism by the SEC and stakeholders, we observed a decrease in boilerplate language when comparing pre-breach cybersecurity disclosures to disclosures made in the year of the breach and in subsequent years. This finding—a significant decrease in boilerplate language following a cyber breach—

*The authors are with Lamar University, Beaumont, Texas.

is our contribution to the accounting literature. This study suggests, based on boilerplate language usage, that firms do not appear to follow the SEC guidance on cybersecurity disclosures until a breach occurs.

Part II of this article provides the background on textual analysis of financial statement disclosures in the existing accounting literature. Part III applies the textual analysis measures from prior research (i.e., fog, length, specificity, boilerplate, and tone) to develop our hypothesis considering our variable of interest, the occurrence of a cyber breach. Part IV describes our methodology discusses our results. We ultimately conclude that the occurrence of a cybersecurity breach has a significant impact on the use of boilerplate language and the length of cybersecurity disclosures.

II. Prior Literature

Over the past two decades, textual analysis in accounting primarily focused on annual reports in the public sector. This body of research examines one of three aspects of financial disclosures: the amount of disclosure, the tone, and/or the transparency (readability) of the report (Li, 2010). The amount of disclosure addresses the physical length of an annual report and researchers often use it as a proxy for the complexity or readability of the report (Peterson, 2012; Lee, 2012; Leuz & Schrand, 2009; Miller, 2010). Research on the tone of financial disclosures in accounting can employ one of two methods: a rules-based or "dictionary" approach, which classifies text into different categories based on specific rules, or a statistical approach that examines the correlations between the text and the document type (Jurafsky and Martin, 2014; Mitchell 2006). Studies employing readability measures offer a more refined approach than the amount of disclosure does, often measuring the reading level based on the complexity of the content.

This study adopts the dictionary approach and uses the Linguistic Inquiry and Word Count (LIWC) software to analyze the tone, language metrics, and cognitive processes of annual financial reports.[1] Using this approach, we aim to differentiate between the use of these three dimensions of textual content before and after cybersecurity breaches. Our goal is to determine how does a cyber breach impacts cybersecurity disclosures. Specifically, we seek to identify if there are significant differences in content before and after a breach. We also consider if there are differences in pre-breach periods and breach periods when analyzed in isolation. We attempt to answer these questions through a content analysis of the financial reports from U.S. firms that experienced a cybersecurity breach.

Leuz and Schrand (2009) examine the link between disclosure and the cost of capital for firms that experienced an exogenous cost of capital shock after the Enron scandal. They find that firms respond to this shock by expanding the number of pages in their 10-K filings and by providing additional interim disclosures, such as conference calls and 8-K filings. They also note that this observation is more pronounced for firms with larger financing needs and positive cost of capital shocks.

Research on the effect of cybersecurity breaches in accounting is limited. Gordon et al. (2015) find that information sharing reduces firms' tendency to defer cybersecurity investments. They also note that cybersecurity measures are crucial for a firm to "maintain the integrity of its external and internal financial reports," a notion that the SEC backs with its guidance on cybersecurity disclosures. Another strand of research examines the risks associated with hackers (Hausken, 2017; Smith and Rupp, 2002), and information sharing related to cybersecurity incidents (He et al., 2018; Laube and Böhme, 2017). Other studies focus on assessing and responding to cyber breaches in specific industries (Apostolou, Apostolou, and Schaupp, 2018). These areas of research support the need to provide meaningful cybersecurity risk disclosures in the firms' Management Discussion and Analysis section of the annual report (MD&A).

III. Hypothesis Development

The Verizon DBIR (2016) defines a cybersecurity incident as an event that compromises the integrity, confidentiality, or availability of an information asset. A cybersecurity breach is an incident that results in the confirmed disclosure of data to an unauthorized party. In this study, we examine the impact of cybersecurity breaches on the content of cybersecurity disclosures. Our hypothesis considers five variables used in prior literature which are interest to investors, users of financial statements, and regulators: length, boilerplate, fog, specificity, and tone.

a. Length

Prior literature has analyzed effect of exogenous shocks on the length of financial statements disclosures. For instance, Lang and Stice-Lawrence (2015) find that IFRS adoption had a significant impact on the length of financial

[1] Psychologist James W. Pennebaker from the University of Texas created the Linguistic Inquiry and Word Count software (LIWC). It is available for public use online at https://liwc.wpengine.com.

statement disclosures by increasing length. Morunga & Bradbury (2012) also found an increase in length of financial statement disclosures of firms in New Zealand upon adoption of IFRS. Leuz and Schrand (2009) observed that firms extended the length of financial statement disclosures, particularly in the MD&A section, in response to the cost of capital shock during the Enron event period.

Overall, we expect to observe the same effect of a cyber breach on the length of disclosures: firms will provide lengthier disclosures that include details about the breach and discuss the effects of the breach on the firm. We also expect that length will increase because firms are likely to increase disclosures related to internal controls in response to a breach.

H1: The occurrence of a cyber breach increases the length of disclosures.

b. Boilerplate

The academic literature and regulators have considered the use of boilerplate language in financial statements disclosures. For purposes of this study, we follow Dyer, Lang, and Stice-Lawrence (2017) and refer to boilerplate as consisting of "generic and standardized disclosures" and "re-use of the same firm's disclosure from a prior period." Lang and Stice-Lawrence (2014) considered the effect of IFRS adoption on the use of boilerplate in annual reports and the relationship between boilerplate and predetermined economic outcomes. Their study found that adoption of IFRS reduced boilerplate and that textual attributes such as boilerplate are correlated with liquidity, analyst following, and mutual fund ownership. McClane (2019) studied the use of boilerplate in securities deal making and found that boilerplate disclosures increase IPO costs for firms in the aggregate, but some issuers may find the additional costs worth paying. At the same time, regulators continue to show concern regarding the use of boilerplate with respect to cybersecurity disclosures, and the latest SEC guidance (2018) reiterates that firms should avoid generic disclosures that contain boilerplate.

In general, we expect to observe more boilerplate and generic disclosures in years prior to the occurrence of a cyber breach. However, after the occurrence of a breach, we expect to observe more in-depth analysis of cybersecurity risks and preventive measures and extended discussion of the costs and potential legal liability associated with the occurrence of the breach.

H2: The occurrence of a cyber breach decreases boilerplate language.

c. Fog

Fog represents a measure of the reading level of any given text. According to Li (2008), "the Fog index proposes that, assuming everything else to be equal, more syllables per word or more words per sentence make a document harder to read." Using the Fog index, Li found that the annual reports of firms with lower earnings had a higher fog index (i.e., they were harder to read). Other studies using the Fog index include Biddle, Gilles and Verdi (2009), considering fog to study how financial reporting quality relates to investment efficiency; Miller (2009), using fog to examine the effects financial reporting complexity on investor's trading activity; Lehavy, Li and Merkley (2011), using fog to study the effect of the readability of financial reports on the behavior of financial analysts; Dougal, Engelberg, García, and Parsons (2012), taking into account fog to analyze the effect of financial reporting by journalists and stock market performance; and Lawrence (2013), considering fog to examine how individual investor's holdings vary with respect to the quality of a firm's financial disclosures.

We expect that the occurrence of a cyber breach will be followed by a discussion of technical topics related to information technology, prevention and remediation of cyber risks, legal liabilities, and contingencies, which will likely make disclosures harder to read. These disclosures may contain technical terms related to information technology and multisyllabic words that may be unfamiliar to financial statement users. Furthermore, we expect that closer scrutiny and review of disclosures by management, auditors, attorneys, and other experts following a cyber breach may increase the use of technical language.

H3: The occurrence of a cyber breach increases the level of fog.

d. Specificity

In 2016, specificity was introduced into the academic literature by Hope, Hu and Lu (2016) as a new measure to quantify the specificity in firm's risk-factor disclosures. They construed specificity based on "the number of specific entity names including names of persons, locations and organizations, quantitative values in percentages, money values in dollars, times, and dates scaled by the total number of words in that section." Their study found that market reaction to the filing of a 10-K is positively associated with specificity and that analysts are more able to assess fundamental risks when risk-factors

disclosures are more specific. Based on these findings, they concluded that more specific risk-factor disclosures benefit users of financial statements.

We expect that cybersecurity disclosures will be more specific following a cyber breach as they are more likely to contain specific information describing the occurrence and the effects of the breach, particularly with respect to names of organizations, persons, quantitative values, money values in dollar, times, and dates.

H4: The occurrence of a cyber breach increases the specificity of disclosures.

e. Tone

The tone of financial statement disclosures has been studied in the academic literature to determine its implications on earnings and stock prices. Tetlock (2007) studied the use of positive and negative words by business journalists and found that high media pessimism induce downward pressure on market prices and unusually high or low pessimism predicts high trading volume. Li (2010) used a Bayesian statistical learning approach and found that future earnings and liquidity are better when managers MD&A's disclosures are more optimistic. Studies that examine the tone of financial statement disclosures have considered positive tone, negative tone, and uncertain tone (Feldman et al. 2010, Henry 2008, Kothari et al. 2009, Smith 2017).

We predict that the occurrence of a cyber breach will affect the tone of disclosures. Specifically, we expect to observe an increase in both negative tone and uncertain tone. Conversely, we anticipate a decrease in positive tone. Following a cyber breach, firms will likely report mostly bad news, which would contain pessimistic or uncertain words. Moreover, it is unlikely that management will use positive words to describe a cyber breach due to the risk of misleading investors on the nature, scope, and extent of the breach.

H5: The occurrence of a cyber breach affects tone.

IV. Methodology And Results

Table 1 shows our sample selection process and exclusions to arrive at a final sample of 235 firm years. We begin by analyzing the VERIS Community Database (VCDB), which is the source data of the Verizon DBIR.[2] We then exclude breaches before 2012 and after 2015, to ensure both a wide sample range and that records are available for two years before and after a recorded breach. This sample range is chosen because the 2011 SEC guidance for cybersecurity disclosure did not take effect until 2012.[3] Additionally, complete VCDB breach data are available beginning in 2011. Because breaches can include any amount of data compromised, we limit our sample to large breaches, which we define as at least 1,000 records of personal data compromised because the actual cost of a breach for a firm is rarely provided in the VCDB and is difficult to accurately measure[4]. [See Table 1, pg. 206]

We then exclude firms based on industry, nationality (foreign firms excluded), and those with multiple breaches during the sample period.[5] We also exclude missing data from the sample: firms with 10-Ks not filed with the SEC, missing 10-K years on SEC EDGAR, and 10-Ks without security breach disclosures to arrive at a final sample of 235 firm years.

We employ several textual analysis measures from prior literature: FOG, LENGTH, SPECIFICITY, NEGATIVE, POSITIVE, and UNCERTAIN. Our variable of interest, BREACH, is an indicator variable denoting the year before a breach occurred (0) or a year during or after a breach (1).

---

[2] The VERIS Community Database is publicly available at http://veriscommunity.net/vcdb.html.

[3] Importantly, we decided to limit our study to breaches that occurred after 2011 to ensure that the results of our study reflect the impact of a cybersecurity breach on disclosures as opposed to changes in disclosures due to regulatory changes. Had we included in our study breaches occurring in 2011 or prior years, it is possible that our results would have been impacted by changes in disclosures resulting from compliance with the SEC's guidance on cyber disclosure. Yet, the goal of our study is not to determine the broad impact of regulatory guidance on cyber disclosures.

[4] We chose 1,000 records for a number of reasons: (1) The VCDB lists all breaches regardless of materiality. Many breaches included in the database have very few compromised records. 1,000 records was the chosen cut-off point to ensure that the breaches included in our sample represented a large number of records being compromised while maintaining a statistically significant sample size. (2) There is little cost data in the VDCB. Cost would be an ideal measure, but because it is not available, records are used as a proxy for cost. (3) There is no extant literature on the number of records that will constitute a material breach.

[5] These exclusions were made to ensure 10-Ks were available for each firm year on SEC EDGAR. Additionally, multiple breaches can obscure results as the study is designed to examine textual constructs two years before and after a breach.

As previously stated, our model employs variables used directly in prior literature, most closely following Lang and Stice-Lawrence (2014), Hope et al. (2016), and Smith (2017).

We use the following equation to examine our hypotheses:

$$BREACH_t = \alpha + \beta_1(FOG_t) + \beta_2(LENGTH_t) + \beta_3(BPLAVG_t) + \beta_4(BPLMAX_t) + \beta_5(SPECIFICITY_t) + \beta_6(NEGATIVE_t) + \beta_7(POSITIVE_t) + \beta_8(UNCERTAIN_t) + \varepsilon$$

The Gunning-Fog index (FOG) measures the reading level of any given text using the following formula:
FOG = (words per sentence + percentage of complex words) * 0.4,
where complex words are words with at least three syllables.

We employ the Lingua:EN:Fathom Module in Perl to measure both FOG and LENGTH (Lang and Stice-Lawrence, 2015; Boritz et al., 2016; Bushee et al., 2018). This module analyses English text in a string or text file and computes the FOG index by counting the number of words, sentences, syllables (Lingua:EN:Syllable), and blank and non-blank text. To measure LENGTH, we use the natural logarithm transformation of the word count from Lingua:EN:Fathom to pare down large figures.

Disclosure of cybersecurity risk carries potential value to the users of financial statements when there is uncertainty about the riskiness of the firm's cash flows (Beyer 2009, Heinle and Smith 2017). To examine the consequences of providing more specific cybersecurity risk disclosures, we include SPECIFICITY.

We measure SPECIFICITY following Hope et al. (2016), except we limit our measure to the cybersecurity disclosure section of the 10-K. We define SPECIFICITY as the number of specific words or phrases conveying specific information relevant to the disclosing firm divided by the total words in the cybersecurity disclosure section of the 10-K. We employ Stanford Named Entity Recognizer (NER), an open-source software package, to count the seven entity categories referenced in cybersecurity disclosures: (1) names of locations, (2) names of organizations, (3) dates, (4) time, (5) names of people, (6) percentages, and (7) monetary values in dollars.

There are several common measures of tone in prior literature according to the Loughran McDonald English business dictionary (June 2017 version). These include a measure of negative tone, positive tone, and uncertain tone, among others (Feldman et al. 2010, Henry 2008, Kothari et al. 2009, Smith 2017).[6] We restrict our measures of tone to this dictionary to help us identify tone usage in business writing and avoid including proper nouns or words from foreign languages. We measure NEGATIVE, POSITIVE, and UNCERTAIN using Loughran and McDonald's (2017) three accompanying word dictionaries to capture the cybersecurity disclosure tone.[7] We converted the word lists to text files and extracted them into columns to import them into LIWC for use as a custom dictionary. The negative and uncertainty word dictionaries approximate the level of negative or cybersecurity risk-related content discussed in the 10-K. The positive dictionary captures any usage of tone besides the content in the negative and uncertain dictionaries. We use these dictionaries in the Linguistic Inquiry and Word Count software (LIWC) to analyze the counts of tone. LIWC reports the word counts for any given measure of tone in the dictionary for a given text file. We convert the cybersecurity disclosure portion of the 10-K into a text file and pass it through LIWC for analysis.

Boilerplate disclosure is a common construct in the textual analysis literature (McMullin 2016). Our measure of boilerplate disclosure, BPLAVG, is unique in that we do not compare text to a "corpus," or comprehensive text, to determine whether a disclosure is boilerplate. We employ a plagiarism software, WCopyfind, following prior literature in content analysis to make comparisons between text (Cazier and Pfeiffer 2015, McMullin 2016, Beatty et al. 2019) to make one-to-one comparisons with a firm's own disclosures for the other four years of the sample. WCopyFind compares two documents side-by-side using certain textual parameters such as "shortest phrase to match" and "minimum % of matching words" to measure the aggregate percentage of plagiarism between the two documents.[8] These results produce a matrix for each firm's

[6] Other measures of tone the Loughran McDonald English business dictionary offers include litigious, modal, and constraining. For more information on the business dictionary, see https://sraf.nd.edu/.

[7] There are 82,834 negative words, 4,727 positive words, and 24,993 uncertain words in the Loughran McDonald Master Dictionary.

[8] We use WCopyfind version 4.1.5 - Windows 64 Bit, which allows the following "comparison rules" for plagiarism measurement: Shortest phrase to match, fewest matches to report, most imperfections to allow, minimum % of matching words, ignore all punctuation, ignore outer punctuation, ignore numbers, ignore letter case, skip non-words, skip words longer than X characters, and basic characters only. We employ the shortest phrase to match as four words, with a minimum match to report as four, ignored all punctuation, and ignored all numbers.

disclosure, where each year of the five sample years has four unique results. We take these plagiarism percentages for each firm year and average them across the four years, and then assign this figure to BPLAVG, or the average boilerplate figure when comparing a single firm year to the other four firm years. We measure BPLMAX as the maximum boilerplate disclosure within the matrix. We adopt this unique methodology for several reasons. First, there is no defined corpus in the existing literature on cybersecurity breaches. Second, we want to compare a firm's post-breach disclosure to itself rather than to other firms' disclosures. Not all firms had uninformative boilerplate pre-breach disclosures, and our goal was to have a measure of how each individual firm changed its disclosures after the occurrence of a breach. Third, because we have a matrix of results, an average seemed most appropriate. We chose to employ two pre-breach and two post-breach years, so choosing a single breach year and running a plagiarism test with a single pre-breach year would produce an inaccurate boilerplate measure.

Results

Table 2 presents the descriptive statistics for 47 unique firms over the five-year sample period. The mean FOG index indicates that the cybersecurity disclosure portion of the MD&A is at a college graduate reading level, with an index of 17 or above (mean 25.19). FOG is high for these disclosures most likely due to the nature of the disclosure. This text includes policies for addressing cybersecurity threats, preventative actions taken, legal statements, exposure to cybersecurity risk, and the effects of cybersecurity breaches. Thus, the percent of complex words in each sentence is relatively high compared to the rest of the 10-K. The mean boilerplate disclosure (BPLAVG) is 0.68, with a measure at the 25th percentile of 0.5625 and 75th percentile of 0.8475. This result indicates a high percentage of boilerplate usage from year to year relative to the full cybersecurity disclosure when comparing disclosures among the five sample years for a firm that experienced a cybersecurity breach. This result appears primarily in non-breach years, where we observe many firms employing a similar statement, or even an exact copy, of their cybersecurity disclosure from prior years. [See Table 2, pg. 206]

Table 3 presents the Pearson and Spearman correlation coefficients for our sample of 235 cybersecurity disclosures. Following the observation of a high BPLAVG, we find a negative correlation between BPLAVG and LENGTH. As cybersecurity disclosures increase in length, most likely due to a change in policy or a cybersecurity breach, their BPLAVG tends to be lower. Not surprisingly, we also observe a negative correlation between BPLAVG and our measure of specificity: thus, less specific text tends to indicate a more boilerplate disclosure. FOG and NEGATIVE have a positive correlation, suggesting that firms with bad news to deliver tend to increase the complexity of their disclosure[9]. [See Table 3, pg. 207]

Table 4 presents the test of our five hypotheses on cybersecurity breach disclosure. As expected, material breaches significantly impact LENGTH, BPLAVG, and BPLMAX. We find that as breaches occur, firms increase the number of words in their cybersecurity disclosure, as indicated by a positive and significant coefficient on LENGTH (p = .0025, .1751), providing support for H1. This result is observed for two reasons: (1) firms increase the amount of disclosure to describe the impact of a cybersecurity breach and (2) boilerplate pre-breach disclosures are typically identical (copy-and-pasted) legal statements, and as boilerplate decreases, LENGTH should correspondingly increase. The results confirm this conjecture, with a negative and significant coefficient on BPLAVG (p = .0026, -.6271), providing support for H2. This finding shows that, as firms experience a cybersecurity breach, they decrease their boilerplate disclosure in both the breach year and the two years following a breach. As mentioned previously, we measure BPLAVG as a percentage. Because we measure our independent variable BREACH as a dummy variable, we can interpret this result as indicating a 62.71% decrease in boilerplate disclosure for breach years and post-breach years from the two pre-breach years. This finding means that firms provide far less boilerplate disclosure in breach years relative to pre-breach years. Finally, we find that the BPLMAX is increasing in breach years. While unexpected, this increase could be due to the nature of BPLMAX compared to BPLAVG. BPLMAX takes the maximum observation from the matrix of boilerplate percentages, and this figure can be as high, if not higher, in years four and five (post-breach) compared to years one and two (pre-breach). The breach year, year three, is often not the cause of the high maximum boilerplate in breach years. [See Table 4, pg. 207]

We find that cybersecurity breaches have no significant impact on the level of FOG. The FOG measure is high (mean = 25.1918) for both pre-breach and breach disclosures in the MD&A, with a college graduate reading level required in both cases (FOG > 17). Because FOG is already well above the college reading level, we are unlikely to find increases

[9] Collinearity tests were run for the variance inflation factors (VIFs) for all variables. In untabulated results, the VIFs for all variables were less than 3, with the highest observation being BPLMAX at 2.200 followed by BPLAVG at 2.176. Because these VIFs are less than 10, they are considered relatively weak predictors of the other independent variables, as noted in prior literature (Menard 1995).

in FOG. The complexity of disclosure begins high, and material breaches do not impact the level of FOG, likely due to the legal nature of the disclosure. We also find that cybersecurity breaches have no significant impact on SPECIFICITY or the three measures of tone (POSITIVE, NEGATIVE, UNCERTAIN). Based on these findings, we found no support for H3, H4, or H5.

V. Conclusions

Cybersecurity incidents have increased exponentially, with many U.S. public companies disclosing breaches to their information systems. These breaches compromise assets and customer information affect corporate reputation, and result in significant remediation costs and legal contingencies. Investors, customers, and the general public are growing more concerned about cybersecurity, demanding more information on these incidents, particularly those involving actual breaches. Against this backdrop, the SEC has issued two interpretive sets of guidance on cybersecurity disclosures that discourage the use of boilerplate language and emphasize the need to provide clearer and more robust disclosures that adequately inform investors about cybersecurity risks and incidents.

We employed content analysis to examine whether the occurrence of a cyber breach affects M&D disclosures on cybersecurity. Specifically, we aimed to determine if there are significant differences in content before and after a breach and if there are differences in pre-breach periods and post-breach periods when analyzed in isolation. We sought to answer these questions with a content analysis of 235 cybersecurity disclosures by 47 firms that experienced a cybersecurity breach over a five-year period. Our results suggest that cyber breaches have a significant impact on the length the disclosures, as we observed a 17.5% increase in the number of words in cybersecurity disclosures following a breach. We also observed a 62.71% decrease in boilerplate language when comparing pre-breach cybersecurity disclosures to disclosures made in the year of the breach and in subsequent years. The support found for our hypothesis regarding a decrease in the use of boilerplate language is our contribution to the accounting literature. Firms have shown, based on boilerplate language usage, that SEC guidance is generally not heeded until breaches occur, at which point cybersecurity disclosures more accurately represent the content set forth in the guidance. Conversely, we found that cybersecurity breaches have no significant impact on FOG, arguably because the complexity of disclosures was already high prior to the breach. We were not able to establish a significant difference with respect to the tone of disclosures, despite observing a 6% decrease in the use of words associated with a positive tone.

Our conclusions are subject to limitations. First, the SEC issued its first official guidance on disclosures related to cybersecurity breaches and incidents in October 2011; therefore, we limited our sample period to public disclosures occurring on or after 2012. Second, our findings do not account for the materiality of a cybersecurity breach on the content of disclosures. Third, our findings do not consider the potential relationship between the type of cybersecurity incident (*e.g.*, hacking, malware, stolen credentials, cyber espionage) and the content of disclosures. Fourth, companies may be motivated to provide vague or minimal cybersecurity disclosures to protect themselves from actors who may otherwise be able to exploit threats or overcome cybersecurity barriers. We limited our sample to reports issued by public registrants in the U.S. and did not contemplate the effect of cybersecurity incidents on financial statements in other countries. Lastly, our study does not consider the effects of the new SEC interpretive guidance issued on February 26, 2018, titled, "*Statement on Guidance on Public Company Cybersecurity Disclosures*" on the content of cybersecurity disclosures issued on or after 2018.

While our research is a first step in studying the effects of cybersecurity breaches on the content of disclosures, future research could evaluate the important relationship between materiality and the content of cybersecurity disclosure. The disclosure obligations of U.S. registrants are based on materiality, and there are reports that U.S. firms have sometimes failed to report cybersecurity incidents to investors on the grounds that they are not material. Likewise, future research could study the content of cybersecurity disclosures to develop ratings and benchmarks for the quality and quantity of disclosures, which could be useful to investors who may wish to reduce their loss exposure due to cybersecurity threats and incidents.

References

American Institute of Certified Public Accountants (AICPA). 2017. *Cybersecurity Risk Security Management Reporting Framework*. Durham, N.C.: AICPA.

Apostolou, B., Apostolou, N., and Schaupp, L. (2018). Assessing and Responding to Cyber Risk: The Energy Industry as Example. *Journal of Forensic and Investigative Accounting*, *10*(1), 73–86.

Beatty, A., Cheng, L., and Zhang, H. (2019). Are risk factor disclosures still relevant? Evidence from market reactions to risk factor disclosures before and after the financial crisis. *Contemporary Accounting Research, 36*(2), 805–838.

Beyer, A. (2009). Capital market prices, management forecasts, and earnings management. *The Accounting Review, 84*(6), 1713–1747.

Biddle, G., Gilles, H., and Verdi, R. (2009). How does financial reporting quality relate to investment efficiency? Journal of Accounting and Economics, *48*, 112–131.

Boritz, J. E., Hayes, L., and Timoshenko, L. M. (2016). Determinants of the readability of SOX 404 reports. *Journal of Emerging Technologies in Accounting*, *13*(2), 145–168.

Bushee, B. J., Gow, I. D., and Taylor, D. J. (2018). Linguistic complexity in firm disclosures: obfuscation or information? *Journal of Accounting Research*, *56*(1), 85–121.

Cazier, R. A., and Pfeiffer, R. J. (2015). Why are 10-K filings so long? *Accounting Horizons*, *30(*1), 1–21.

Dougal, C., Engelberg, J., Garcia, D., and Parsons, C. (2012). Journalists and the stock market. *Review of Financial Studies*, 25, 639–679.

Dyer, T., Lang, M., and Stice-Lawrence, L. (2017). The evolution of 10-K textual disclosure: Evidence from Latent Dirichlet Allocation. *Journal of Accounting and Economics*, 64(2), 221–245.

Feldman, R., Govindaraj, J., Livnat, J., and Segal, B. (2010). Management's tone change, post earnings announcement drift and accruals. *Review of accounting studies*, *15*(4), 915–953.

Ferraro, M. (2014). Groundbreaking or broken? An analysis of SEC cybersecurity disclosure guidance, its effectiveness, and implications. Albany Law Review 77, 297–347.

Gordon, L. A., Loeb, M. P., Lucyshyn, W., and Zhou, L. (2015). The impact of information sharing on cybersecurity underinvestment: a real options perspective. *Journal of Accounting and Public Policy*, *34*(5), 509–519.

Hausken, K. (2017). Information sharing among cyber hackers in successive attacks. *International Game Theory Review*, *19*(02), 1750010.

He, M., Devine, L., and Zhuang, J. (2018). Perspectives on cybersecurity information sharing among multiple stakeholders using a decision-theoretic approach. *Risk Analysis, 38*(2), 215–225.

Heinle, M., and Smith, K. (2017). A theory of risk disclosure. *Review of Accounting Studies*, *22*(4), 1459–1491.

Henry, E. (2008). Are investors influenced by how earnings press releases are written? *Journal of Business Communication 45*, 363–407.

Hope, O., Hu, D. and Lu, H. (2016). The benefits of specific risk-factor disclosures. *Review of Accounting Studies* 21(4), 1005–1045.

Jurafsky, D., and Martin, J. H. (2014). *Speech and language processing* (Vol. 3). London: Pearson.

Kothari, S.P., Li, X., and Short, J.E. (2009). The effect of disclosures by management, analysts, and financial press on the equity cost of capital: A study using content analysis. *The Accounting Review*, *84*, 1639–1670.

Lang, M., and Stice-Lawrence, L. (2015). Textual analysis and international financial reporting: large sample evidence. *Journal of Accounting and Economics*, *60*(2-3), 110–135.

Laube, S., and Böhme, R. (2017). Strategic aspects of cyber risk information sharing. *ACM Computing Surveys (CSUR)*, *50*(5), 77.

Lawrence, A. (2013) Individual investors and financial disclosure. *Journal of Accounting and Economics*, *56*, 130–147.

Lee, Y. J. (2012). The effect of quarterly report readability on information efficiency of stock prices. *Contemporary Accounting Research*, *29*(4), 1137–1170.

Lehavy, R., Feng L., and Merkley, K. (2011). The effect of annual report readability on analyst following and the properties of their earnings forecasts. *Accounting Review*, 86, 1087–1115.

Leuz, C., and Schrand, C. (2009). *Disclosure and the cost of capital: Evidence from firms' responses to the Enron shock* (No. w14897). National Bureau of Economic Research.

Li, F. (2008). Annual report readability, current earnings, and earnings persistence. *Journal of Accounting and Economics*, 45, 221–247.

Li, F. (2010). The information content of forward-looking statements in corporate filings – A naïve Bayesian machine learning approach. *Journal of Accounting Research*, 48, 1049–1102.

McClane (2019). Boilerplate and the impact of disclosure in securities deal making. *Vanderbilt Law Review*, *72*(1), 191–295.

McMullin, J. (2016). Can I borrow your footnotes? Footnote boilerplate's learning externality.

Menard, S. (1995). *Applied Logistic Regression Analysis*: Sage University Series on

Quantitative Applications in the Social Sciences. Thousand Oaks, CA: Sage.

Miller, B. P. (2010). The effects of reporting complexity on small and large investor trading. *The Accounting Review*, *85*(6), 2107–2143.

Mitchell, T. M. (2006). *The discipline of machine learning* (Vol. 3). Carnegie Mellon University, School of Computer Science, Machine Learning Department.

Morunga, M., and Bradbury, M. (2012). The impact of IFRS on annual report length. *Australasian Accounting, Business and Finance Journal*, 6(5), 47–62.

Peterson, K. (2012). Accounting complexity, misreporting, and the consequences of misreporting. *Review of accounting studies*, *17*(1), 72–95.

Securities and Exchange Commission (SEC). 2011. *Cybersecurity*. Corporation Finance Disclosure Guidance: Topic No. 2. Washington, D.C.: SEC.

Securities and Exchange Commission (SEC). 2018. *Commission statement and guidance on public company cybersecurity disclosures.* Release Nos. 33-10459; 34-82746. Washington, D.C.: SEC.

Schatz, D., Bashroush, R., and Wall, J. (2017). Towards a more representative definition of cyber security. *Journal of Digital Forensics, Security and Law*, *12*, 52–74.

Smith, K. (2017). Tell me more: A content analysis of expanded auditor reporting in the United Kingdom. Available at SSRN: https://ssrn.com/abstract=2821399 or http://dx.doi.org/10.2139/ssrn.2821399.

Smith, A. D., and Rupp, W. T. (2002). Issues in cybersecurity; understanding the potential risks associated with hackers/crackers. *Information Management and Computer Security*, *10*(4), 178–183.

Tetlock, P. (2007). Giving content to investor sentiment: the role of media in the stock market. *Journal of Finance*, 62, 1139–1168.

Tuma, S., and Rucker, J. (2018). Privileges: Understanding applicability in cybersecurity cases, *Texas Bar Journal*, 690–692.

Verizon Business RISK Team. (2016). *Verizon 2016 Data Breach Investigations Report*. New York City, NY. Verizon Communications, LLC.

Table 1: Sample Selection

Total records in the VERIS Community Database	7,789
Breaches before 2012 and after 2015	(2,701)
Breaches with compromised data size < 1,000 records	(3,922)
Breaches in public, educational, or healthcare industries	(807)
Foreign firms	(167)
Non-public firms (manual search)	(111)
Repeated firms (firms with multiple breaches)	(14)
Firms with 10-Ks not filed on SEC EDGAR	(25)
Firms Subtotal	42
Add: Firms directly mentioned in DBIR (filing on SEC)	10
Total firms	52
Number of years to obtain 10-K	5
Total possible 10-Ks	260
Less: Missing 10-K years	(15)
Sample Subtotal	245
10-Ks without security breach disclosure	(10)
Firm years	235

Table 2: Descriptive Results (N= 235)

Variable	Mean	Std Dev	25th %-ile	Median	75th %-ile
BREACH	0.6426	0.4803	0.0000	1.0000	1.0000
FOG	25.1918	2.9712	22.6216	25.2157	27.3587
LENGTH	6.1822	0.7068	5.6733	6.1717	6.7441
BPLAVG	0.6818	0.2176	0.5625	0.7100	0.8475
BPLMAX	0.8713	0.1897	0.8400	0.9500	0.9900
SPECIFICITY	6.0511	11.5646	0.0000	1.0000	7.0000
NEGATIVE	8.1335	1.9256	6.7800	8.1000	9.2700
POSITIVE	0.6454	0.5115	0.2900	0.5400	0.9000
UNCERTAIN	3.0532	0.9060	2.4400	3.0400	3.5300

Table 3: Pearson/Spearman Correlation Coefficients N = 235

	BREACH	FOG	LENGTH	BPLAVG	BPLMAX	SPECIFICITY	NEGATIVE	POSITIVE	UNCERTAIN
BREACH	1	0.01	0.19	-0.12	0.06	0.13	-0.07	0.02	-0.05
		0.84	0.00	0.07	0.33	0.05	0.32	0.72	0.42
FOG	0.00	1	-0.21	0.04	0.04	-0.26	0.26	0.00	-0.14
	0.98		0.00	0.51	0.53	<.0001	<.0001	0.98	0.03
LENGTH	0.20	-0.20	1	-0.18	-0.30	0.63	-0.48	0.20	-0.11
	0.00	0.00		0.00	<.0001	<.0001	<.0001	0.00	0.08
BPLAVG	-0.09	0.06	-0.19	1	0.60	-0.19	0.08	-0.15	-0.04
	0.15	0.38	0.00		<.0001	0.00	0.23	0.02	0.57
BPLMAX	0.07	0.00	-0.16	0.73	1	-0.30	0.18	-0.04	0.05
	0.31	0.99	0.02	<.0001		<.0001	0.01	0.51	0.45
SPECIFICITY	0.08	-0.23	0.55	-0.28	-0.29	1	-0.51	0.04	-0.14
	0.22	0.00	<.0001	<.0001	<.0001		<.0001	0.51	0.03
NEGATIVE	-0.08	0.23	-0.52	0.06	0.03	-0.37	1	-0.34	0.32
	0.25	0.00	<.0001	0.32	0.67	<.0001		<.0001	<.0001
POSITIVE	0.01	0.04	0.20	-0.03	0.05	-0.06	-0.33	1	-0.19
	0.90	0.53	0.00	0.69	0.49	0.39	<.0001		0.00
UNCERTAIN	-0.06	-0.14	-0.15	0.05	0.07	-0.25	0.31	-0.22	1
	0.39	0.03	0.02	0.49	0.29	<.0001	<.0001	0.00	

Spearman correlations are represented in the upper right half of the table, with Pearson correlations on the bottom left half of the table.

Table 4: Impact of Breaches on Textual Characteristics of Cybersecurity Disclosures (N = 235)

Variable	**Parameter Estimate**	**Standard Error**	**t Value**	**Pr > |t|**
FOG	0.0065	0.0111	0.59	0.5562
LENGTH	0.1751***	0.0574	3.05	0.0025
BPLAVG	-0.6271***	0.2059	-3.05	0.0026
BPLMAX	0.7720***	0.2375	3.25	0.0013
SPECIFICITY	-0.0020	0.0035	-0.57	0.5700
NEGATIVE	0.0089	0.0204	0.43	0.6642
POSITIVE	-0.0662	0.0664	-1	0.3197
UNCERTAIN	-0.0314	0.0377	-0.83	0.4060

***,**, and * indicate significance at the .01, .05, and .10 levels, respectively.

Appendix A: Target 2013 10-K Pre-Breach Cybersecurity Disclosure

If our efforts to protect the security of personal information about our guests and team members are unsuccessful, we could be subject to costly government enforcement actions and private litigation and our reputation could suffer.

The nature of our business involves the receipt and storage of personal information about our guests and team members. We have a program in place to detect and respond to data security incidents. To date, all incidents we have experienced have been insignificant. If we experience a significant data security breach or fail to detect and appropriately respond to a significant data security breach, we could be exposed to government enforcement actions and private litigation. In addition, our guests could lose confidence in our ability to protect their personal information, which could cause them to discontinue usage of REDcards, decline to use our pharmacy services, or stop shopping with us altogether. The loss of confidence from a significant data security breach involving team members could hurt our reputation, cause team member recruiting and retention challenges, increase our labor costs and affect how we operate our business.

A significant disruption in our computer systems could adversely affect our operations.

We rely extensively on our computer systems to manage inventory, process guest transactions, service REDcard accounts and summarize and analyze results. Our systems are subject to damage or interruption from power outages, telecommunications failures, computer viruses and malicious attacks, security breaches and catastrophic events. If our systems are damaged or fail to function properly, we may incur substantial costs to repair or replace them, experience loss of critical data and interruptions or delays in our ability to manage inventories or process guest transactions, and encounter a loss of guest confidence which could adversely affect our results of operations.

Appendix B: Target 2014 10-K Post-Breach Cybersecurity Disclosure

The data breach we experienced in 2013 has resulted in government inquiries and private litigation, and if our efforts to protect the security of information about our guests and team members are unsuccessful, future issues may result in additional costly government enforcement actions and private litigation and our sales and reputation could suffer.

The nature of our business involves the receipt and storage of information about our guests and team members. We have a program in place to detect and respond to data security incidents. However, because the techniques used to obtain unauthorized access, disable or degrade service, or sabotage systems change frequently and may be difficult to detect for long periods of time, we may be unable to anticipate these techniques or implement adequate preventive measures. In addition, hardware, software or applications we develop or procure from third parties may contain defects in design or manufacture or other problems that could unexpectedly compromise information security. Unauthorized parties also may attempt to gain access to our systems or facilities through fraud, trickery or other forms of deceiving our team members, contractors and temporary staff. Until the fourth quarter of 2013, all incidents we experienced were insignificant. The Data Breach we experienced was significant and went undetected for several weeks. We experienced weaker than expected U.S. Segment sales immediately following the announcement of the Data Breach, and we are currently facing more than 80 civil lawsuits filed on behalf of guests, payment card issuing banks and shareholders. In addition, state and federal agencies, including State Attorneys General, the Federal Trade Commission and the SEC, are investigating events related to the Data Breach, including how it occurred, its consequences and our responses. Those claims and investigations may have an adverse effect on how we operate our business and our results of operations.

If we experience additional significant data security breaches or fail to detect and appropriately respond to significant data security breaches, we could be exposed to additional government enforcement actions and private litigation. In addition, our guests could further lose confidence in our ability to protect their information, which could cause them to discontinue using our REDcards or pharmacy services or stop shopping with us altogether.

A significant disruption in our computer systems and our inability to adequately maintain and update those systems could adversely affect our operations and our ability to maintain guest confidence.

We rely extensively on our computer systems to manage inventory, process guest transactions, manage guest data, communicate with our vendors and other third parties, service REDcard accounts and summarize and analyze results, and on continued and unimpeded access to the internet to use our computer systems. Our systems are subject to damage or interruption from power outages, telecommunications failures, computer viruses and malicious attacks, security breaches and catastrophic events. If our systems are damaged or fail to function properly, we may incur substantial repair or replacement costs, experience data loss and impediments to our ability to manage inventories or process guest transactions, and encounter lost guest confidence, which could adversely affect our results of operations. The Data Breach we experienced negatively impacted our ability to timely handle customer inquiries, and we experienced weaker than expected U.S. Segment sales following the announcement of the Data Breach.

We continually make significant technology investments that will help maintain and update our existing computer systems. Implementing significant system changes increases the risk of computer system disruption. Additionally, the potential problems and interruptions associated with implementing technology initiatives could disrupt or reduce our operational efficiency and could impact the guest experience and guest confidence.

We experienced a significant data security breach in the fourth quarter of fiscal 2013 and are not yet able to determine the full extent of its impact and the impact of government investigations and private litigation on our results of operations, which could be material.

The Data Breach we experienced involved the theft of certain payment card and guest information through unauthorized access to our network. Our investigation of the matter is ongoing, and it is possible that we will identify additional information that was accessed or stolen, which could materially worsen the losses and reputational damage we have experienced. For example, when the intrusion was initially identified, we thought the information stolen was limited to payment card information, but later discovered that other guest information also was stolen.

We are currently subject to a number of governmental investigations and private litigation and other claims relating to the Data Breach, and in the future, we may be subject to additional investigations and claims of this sort. These investigations and claims could have a material adverse impact on our results of operations or profitability. Our financial liability arising

from such investigations and claims will depend on many factors, one of which is whether, at the time of the Data Breach, the portion of our network that handles payment card data was in compliance with applicable payment card industry standards. While that portion of our network was determined to be compliant by an independent third-party assessor in the fall of 2013, we expect the forensic investigator working on behalf of the payment card networks to claim that we were not in compliance. Another factor is whether, and if so to what extent, any fraud losses or other expenses experienced by cardholders, card issuers and/or the payment card networks on or with respect to the payment card accounts affected by the Data Breach can be properly attributed to the Data Breach and whether, and if so to what extent, it would in any event be our legal responsibility. In addition, the governmental agencies investigating the Data Breach may seek to impose on us fines and/or other monetary relief and/or injunctive relief that could materially increase our data security costs, adversely impact how we operate our network and collect and use guest information, and put us at a competitive disadvantage with other retailers.

Finally, we believe that the greatest risk to our business arising out of the Data Breach is the negative impact on our reputation and loss of confidence of our guests, as well as the possibility of decreased participation in our REDcards Rewards loyalty program which our internal analysis has indicated drives meaningful incremental sales. We experienced weaker than expected U.S. Segment sales after the announcement of the Data Breach, but are unable to determine whether there will be a long-term impact to our relationship with our guests or whether we will need to engage in significant promotional or other activities to regain their trust, which could have a material adverse impact on our results of operations or profitability.

Item 7. Management's Discussion and Analysis of Financial Condition and Results of Operations

Data Breach

Description of Event

As previously disclosed, we experienced a data breach in which an intruder stole certain payment card and other guest information from our network (the Data Breach). Based on our investigation to date, we believe that the intruder accessed and stole payment card data from approximately 40 million credit and debit card accounts of guests who shopped at our U.S. stores between November 27 and December 15, 2013, through malware installed on our point-of-sale system in our U.S. stores. On December 15, we removed the malware from virtually all registers in our U.S. stores. Payment card data used in transactions made by 56 additional guests in the period between December 16 and December 17 was stolen prior to our disabling malware on one additional register that was disconnected from our system when we completed the initial malware removal on December 15. In addition, the intruder stole certain guest information, including names, mailing addresses, phone numbers or email addresses, for up to 70 million individuals. Our investigation of the matter is ongoing, and we are supporting law enforcement efforts to identify the responsible parties.

Expenses Incurred and Amounts Accrued

In the fourth quarter of 2013, we recorded $61 million of pretax Data Breach-related expenses, and expected insurance proceeds of $44 million, for net expenses of $17 million ($11 million after tax), or $0.02 per diluted share. These expenses were included in our Consolidated Statements of Operations as Selling, General and Administrative Expenses (SG&A), but were not part of our segment results. Expenses include costs to investigate the Data Breach, provide credit-monitoring services to our guests, increase staffing in our call centers, and procure legal and other professional services.

The $61 million of fourth quarter expenses also includes an accrual related to the expected payment card networks' claims by reason of the Data Breach. The ultimate amount of these claims will likely include amounts for incremental counterfeit fraud losses and non-ordinary course operating expenses (such as card reissuance costs) that the payment card networks believe they or their issuing banks have incurred. In order for us to have liability for such claims, we believe that a court would have to find among other things that (1) at the time of the Data Breach the portion of our network that handles payment card data was noncompliant with applicable data security standards in a manner that contributed to the Data Breach, and (2) the network operating rules around reimbursement of operating costs and counterfeit fraud losses are enforceable. While an independent third-party assessor found the portion of our network that handles payment card data to be compliant with applicable data security standards in the fall of 2013, we expect the forensic investigator working on behalf of the payment card networks nonetheless to claim that we were not in compliance with those standards at the time of the Data Breach. We base that expectation on our understanding that, in cases like ours where prior to a data breach the entity suffering the breach had been found by an independent third-party assessor to be fully compliant with those standards, the

network-approved forensic investigator nonetheless regularly claims that the breached entity was not in fact compliant with those standards. As a result, we believe it is probable that the payment card networks will make claims against us. We expect to dispute the payment card networks' anticipated claims, and we think it is likely that our disputes would lead to settlement negotiations consistent with the experience of other entities that have suffered similar payment card breaches. We believe such negotiations would effect a combined settlement of both the payment card networks' counterfeit fraud loss allegations and their non-ordinary course operating expense allegations. We based our year-end accrual on the expectation of reaching negotiated settlements of the payment card networks' anticipated claims and not on any determination that it is probable we would be found liable on these claims were they to be litigated. Currently, we can only reasonably estimate a loss associated with settlements of the networks' expected claims for non-ordinary course operating expenses. The year-end accrual does not include any amounts associated with the networks' expected claims for alleged incremental counterfeit fraud losses because the loss associated with settling such claims, while probable in our judgment, is not reasonably estimable, in part because we have not yet received third-party fraud reporting from the payment card networks. We are not able to reasonably estimate a range of possible losses in excess of the year-end accrual related to the expected settlement of the payment card networks' claims because the investigation into the matter is ongoing and there are significant factual and legal issues to be resolved. We believe that the ultimate amount paid on payment card network claims could be material to our results of operations in future periods.

Litigation and Governmental Investigations

In addition, more than 80 actions have been filed in courts in many states and other claims have been or may be asserted against us on behalf of guests, payment card issuing banks, shareholders or others seeking damages or other related relief, allegedly arising out of the Data Breach. State and federal agencies, including the State Attorneys General, the Federal Trade Commission and the SEC are investigating events related to the Data Breach, including how it occurred, its consequences and our responses. Although we are cooperating in these investigations, we may be subject to fines or other obligations, which may have an adverse effect on how we operate our business and our results of operations. While a loss from these matters is reasonably possible, we cannot reasonably estimate a range of possible losses because our investigation into the matter is ongoing, the proceedings remain in the early stages, alleged damages have not been specified, there is uncertainty as to the likelihood of a class or classes being certified or the ultimate size of any class if certified, and there are significant factual and legal issues to be resolved. Further, we do not believe that a loss from these matters is probable; therefore, we have not recorded a loss contingency liability for litigation, claims and governmental investigations in the fourth quarter. See Note 17 of the Notes to Consolidated Financial Statements included in Item 8, Financial Statements and Supplementary Data.

Future Costs

We expect to incur significant investigation, legal and professional services expenses associated with the Data Breach in future periods. We will recognize these expenses as services are received. We also expect to incur additional expenses associated with incremental fraud and reissuance costs on Target REDcards.

Insurance Coverage

To limit our exposure to Data Breach losses, we maintain $100 million of network-security insurance coverage, above a $10 million deductible. This coverage and certain other insurance coverage may reduce our exposure. We will pursue recoveries to the maximum extent available under the policies. As of February 1, 2014, we have recorded a $44 million receivable for costs we believe are reimbursable and probable of recovery under our insurance coverage, which partially offsets the $61 million of expense relating to the Data Breach.

Future Capital Investments

We plan to accelerate a previously planned investment of approximately $100 million to equip our proprietary REDcards and all of our U.S. store card readers with chip-enabled smart-card technology by the first quarter of 2015.

In addition, we may accelerate or make additional investments in our information technology systems, but we are unable to estimate such investments because the nature and scope has not yet been determined. We do not expect such amounts to be material to any fiscal period.

Effect on Sales and Guest Loyalty

We believe the Data Breach adversely affected our fourth quarter U.S. Segment sales. Prior to our December 19, 2013 announcement of the Data Breach, our U.S. Segment fourth quarter comparable sales were positive, followed by meaningfully negative comparable sales results following the announcement. Comparable sales began to recover in January 2014. The collective interaction of year-over-year changes in the retail calendar (e.g., the number of days between Thanksgiving and Christmas), combined with the broad array of competitive, consumer behavioral and weather factors makes any quantification of the precise impact of the Data Breach on sales infeasible.

Fourth quarter sales penetration on our REDcards was 20.9 percent, up 5.4 percentage points from 2012. While the rate of increase slowed following the Data Breach, year-over-year penetration continued to grow.

We know our guests' confidence in Target and the broader U.S. payment system has been shaken. We are committed to, and actively engaged in, activities to restore their confidence. We cannot predict the length or extent of any ongoing impact to sales.