Fall 2015

Cybersecurity disclosure effectiveness on public companies

Jingjing Jin
James Madison University

Cybersecurity Disclosure Effectiveness on Public Companies

An Honors Program Project Presented to

the Faculty of the Undergraduate

College of Business

James Madison University

by Jing Jing Jin

Accepted by the faculty of the Department of Accounting, James Madison University, in partial fulfillment of the requirements for the Honors Program.

FACULTY COMMITTEE:

Project Advisor: Dr. Sandra, Cereola

Reader: Dr. Paul, Copley

Reader: Dr. Timothy, Louwers

HONORS PROGRAM APPROVAL:

Philip Frana, Ph.D.,
Interim Director, Honors Program

PUBLIC PRESENTATION

This work is accepted for presentation, in part or in full, at [venue] **Honors Colloquium** on [date] December 4, 2015.

Table of Contents

Purpose and Objectives

Target Corp. has suffered over $252 million losses since a data breach that occurred in 2013. Because of this breach, Target faces many class-action lawsuits from their stakeholders. In March of 2015, Target offered a $10 million settlement in a data breach lawsuit to implement changes to its security policies (Park, 2015). Target's major data breach is a wake-up call to many companies, particularly companies that rely heavily on electronic information systems. Whether a data breach is caused by a hacker or a by human error, there may be damages that not only impact consumers but also impact the company itself as reputational harm can significantly affect a company's bottom line.

As many companies rely heavily on information technology, the risk of cybersecurity continues to increase (Rahm, 2014). In response to the frequent and severe cybersecurity breaches of publicly traded companies, the Securities and Exchange Commission (SEC) in 2011 issued a financial statement disclosure guidance (SEC, 2011). This disclosure requires public companies to disclose cybersecurity risks and material breaches in their SEC filings. However, this guidance is not a "rule, regulation, or statement" of the SEC (SEC, 2011). SEC Guidance requires public companies to disclose the data breach if it is material – however materiality is never defined – thus leaving the company to decide whether a cybersecurity breach is material or not. If not material, then companies will be at liberty to decide on the amount of information they wish to disclose on the breach in their financial statements.

The Sarbanes-Oxley Act brought new attention to public companies about the concept of materiality (Vorhies, 2005). Materiality is something that will affect investors' decisions, if it impacts the financial statement. In this paper, I will examine public companies' financial statement (10k, 8Q, 10Q) before and after they have suffered a major data breach. The list of companies suffering data breach will be retrieved from the Privacy Rights Clearinghouse (PRC). Some companies have suffered multiple breaches within a year which leads to the question, should they disclose these breaches, even though these breaches independently are not material? In this paper, I am going to discuss what research has been published on cybersecurity breach related issues, and I plan to develop further research questions on cybersecurity disclosure related issues. This study should be of interest to SEC, investors, and other professionals that are concerned with cybersecurity disclosure.

Introduction

On October 13, 2011, the U.S. Securities and Exchange Commission issued a guidance on corporate disclosure of cyber-risks and information security breaches (SEC, 2011). To determine if a company disclosed information on the breach, I reviewed the company's risk factors, management's discussion and analysis of financial conditions and results of operations, description of the business, legal proceedings, financial statement disclosures, and disclosure controls and procedures. However, the disclosure regulations from this guidance are vague and thus do little to force disclosure of valuable information. The guidance has led to companies disclosing ambiguous, generic risk factors that can be applied to any business in any industry (Ferraro, 2014).

If the SEC adopts the guidelines as full-fledged rules, this will eliminate any doubt as to company's responsibilities for disclosure. This should improve transparency in financial statement reporting and improve investor decision making. However, companies tend to limit disclosure of information in their financial statements that may hurt their reputation. Therefore, instead of being proactive, companies will only disclose the minimum of what the SEC requires. In response to reports of major corporate cyber-breaches, the SEC held a "cyber roundtable" in March of 2014 bringing together industry groups and public and private sector participants to discuss whether additional SEC guidance is necessary related to the level of disclosure in a company's public filings (Gotshal, 2015). However, neither the SEC nor its staff has taken any formal action as a follow-up to the March 2014 roundtable.

The goal of this literature review is to report how the SEC guidance has affected disclosure in registrant's financial statements. Relevant research suggests that there is ambiguity in this guidance, which is unclear on materiality. Therefore, companies use their own judgement when deciding whether a breach should be disclosed. Investors require transparency in financial statement reporting. Thus if a company suffers from a material breach, investors will benefit from having the information breach disclosed. The literature review begins with a brief summary of Cybersecurity Disclosure, the impact of a weak definition of materiality, including commentary on the potential harm the "guidance" causes, and the impact of SEC disclosure. The case study of Target is presented in this paper, which sets the context for discussion of cybersecurity disclosure. The review concludes with the gap in the literature review and conclusion.

Literature Review

Cybersecurity Disclosure

The costs of recent data breaches costs have risen by 26% to 11.6 million per company in 2013, (compared to 2012). The total number of breaches in 2013 is 62% greater than in 2012, with a total of over 550 million personal identities exposed, such as credit card information and birth date (Rahm 2014). As reported events of information security breaches increased and Congress pushed for more disclosure regulation from public companies, the SEC issued guidance on October 13, 2011 on corporate disclosure of cyber-risks and information security breaches. Much like other disclosure requirements mandated by federal securities laws, the Disclosure Guidance Topic No. 2 –Cybersecurity (CF DG 2) requires disclosure of significant business risk regarding cybersecurity.

The guidance suggests disclosing the facts and circumstances of specific and material cybersecurity risks. Potential risks include operational, outsourcing, undetected attacks, past occurrences, and insurance coverage (Grant 2014). When determining whether to disclose a breach, the company should consider risk factors, management's discussion and analysis of financial condition and results of operations, description of the business, legal proceedings, financial statement disclosures, and disclosure controls and procedures (Young 2013). In regards to specific attacks, companies should disclose the nature, occurrence, cost, and consequences of the attack. In addition to disclosing the costs of actual attacks, companies should also disclose costs of potential attacks, which can be difficult to estimate, but should include remediation, cybersecurity, lost revenues, regulatory fines, litigation costs, and reputational

damages. Although this disclosure requirement is not a ruling, the guidance can impose sanctions and fines on companies that the SEC deems to be non-compliant (Grant 2014). The purpose of the guidance is to assist public companies in preparing disclosures required by the Securities Act of 1933 and maintain the accurate and complete information in the financial statement. However, the SEC guidance is not legally binding due to vague definitions (Goolsby 2011). The studies that have been done on the materiality of the Cybersecurity breaches disclosure are reviewed below.

Materiality

The Financial Accounting Standards Board (FASB) defined materiality in Financial Accounting Concepts Statement no. 2, Qualitative Characteristics of Accounting Information: "The magnitude of an omission or misstatement of accounting information that, in the light of surrounding circumstances, makes it probable that the judgment of a reasonable person relying on the information would have been changed or influenced by the omission or misstatement" (C, T. G., DePree, Chauncey M.,,Jr, & Grant, G. H., 2000).

In addition to FASB's definition, the SEC issued Staff Accounting Bulletin (SAB) no. 99, which is similar to the interpretation of materiality upheld by the U.S. Supreme Court. Materiality is defined as "a substantial likelihood that the ... fact would have been viewed by the reasonable investor as having significantly altered the `total mix' of information made available" (Basic, Inc. v. Levinson, 485 U.S. 224, 1988). Although FASB and the U.S. Supreme Court define materiality, there are many companies who disclosed general cybersecurity risk with little and vague information.

Stronger definition.

The biggest weakness of the guidance is the requirement of disclosing "material" breaches and the SEC's failure to provide clear guidance. This has lead to many disagreements between the companies and the SEC over their compliance of Disclosure Guidance Topic No. 2 –Cybersecurity (CF DG 2) (Ferraro 2013). The SEC should adapt the guideline as formal rules with specific dollar and percentage of assets thresholds, and with certain protections against unfair hindsight judgement, that will present a significant advancement in the SEC's stated mission of protecting investors and promoting fair and efficient markets (Young 2013). When the definition of materiality is refined, this will eliminate the disagreement between companies and the SEC, and promote the overall goal of the SEC to protect the interest of the stakeholders.

Overreach.

The guidance is limited in its effectiveness because it is just guidance, not a legislative rule, but carries the same weight of authority as the law itself, a clear violation of the Administrative Procedure Act (Ferraro 2013). The issuance of cybersecurity guidance may be an appropriate step for the SEC to take. However, this is a reason for concern about the challenges companies face when disclosing the risk associated with cyber security matters and cyber incidents (Goolsby 2011). Issuance of the Cybersecurity Disclosure guidance increases a company's responsibility by increasing the transparency to the public and increasing cost to protect their cybersecurity.

Impact of the SEC Disclosure.

The SEC Cybersecurity guidance fails to solve the information asymmetry problem between companies and stakeholders. The cybersecurity guidance issued by the SEC procedurally overreaches and substantively underachieves. The guidance overreaches because it is not a legislative rule but carries the same weight as legislation laws. The guidance also underachieves because the disclosure requirements are too vague (Ferraro 2013). Ferraro suggests that SEC should re-evaluate the SEC cybersecurity disclosure guidance and make it into a legislative rule. An improvement to CF DG 2 is needed by issuing it as a legislative rule after the required notice and comment period that would ensure a more sound policy as stakeholders would have the opportunity to weigh in (Ferraro 2013). The requirement to disclose the risk prior to the attack will help stakeholders understand the risk that the company is facing and how the company is remediating past security breaches (Grant 2014).

As a result of the risks and costs, public companies are paying closer attention to cybersecurity including hiring additional IT security personnel, training existing internal agents, and upgrading IT software (Grant 2014). An appropriate cybersecurity oversight plan should include clearly defined roles and responsibilities, recruitment of cybersecurity experts, corporate policies governing cybersecurity, and a regular internal audits of cybersecurity oversight (Lunn 2014). One element of a cybersecurity program may be insurance coverage, because cybersecurity breaches can generate tremendous amounts of loss to a company. Therefore, the insurance is needed to reduce the amount that a company can lose as a result of breaches (Daniel 2014).

Although companies can use cybersecurity insurance to mitigate the risk and reduce the cost, paying close attention to IT governance is the key. It is a legal duty of directors in every publicly traded company. The shareholders can sue directors for any damages resulting from failure to protect cyber-security (Clark 2013). The litigation and enforcement actions are becoming common when a company encounters security breaches of personal information. For example, The Federal Trade Commission filed suit against international hospitality operator Wyndham Worldwide Corp. for “alleged data security failures that led to three data breaches at Wyndham hotels in less than two years” (Trautman 2012).

Although cybersecurity protection is expansive due to unpredictable probability and costs of data breaches, top management has to decide whether to invest heavily in new technology to secure the protection or to purchase cybersecurity insurance (Daniel 2014). It would be to a company’s best interest to protect, improve its IT security and follow SEC requirements to disclose any cybersecurity risks and breaches (Trautman 2012). Overall, it is critical to strengthen cybersecurity and be proactive in data risk management (Sophie 2014). There are advantages and disadvantages for increasing the cybersecurity disclosure regulation, but it will be in the best interest of stakeholders- SEC, investors, and other professionals who are interested in this piece of information.

Gap of the Literature Review

Since SEC Cybersecurity disclosure guidance is a fairly new requirement, there is not much research on this topic. More studies have been done that focus on interpretation of the guidance, rather than the gap of the guidance.

Case Study

In Target's 2014 Financial Statement under Data Security and Privacy Risks section, Target reported the following:

> "We have recorded significant expenses related to the Data Breach. Our losses could exceed the amounts we have recorded by material amounts, and these matters could have a material adverse impact on our results of operations." (Target 2014 10-K, 2015)

Although Target disclosed the 2013 data breach expense on the 2014 10Q report, Target did not report such expenses on the yearend 10-K Income Statement for 2013 data breach expenses. The question remains as to whether or not Target should report data breach expenses on the 10K too.

See Table 1 for Target's 2014 Income Statement and Table 2 for Target's 2014 10-Q Income Statement.

Target 2014 Consolidated Statements of Operations

(millions, except per share data)	2014	2013	2012
Sales	$ 72,618	$ 71,279	$ 71,960
Credit card revenues	—	—	1,341
Total revenues	72,618	71,279	73,301
Cost of sales	51,278	50,039	50,568
Selling, general and administrative expenses	14,676	14,465	14,643
Credit card expenses	—	—	467
Depreciation and amortization	2,129	1,996	2,044
Gain on receivables transaction	—	(391)	(161)
Earnings from continuing operations before interest expense and income taxes	4,535	5,170	5,740
Net interest expense	882	1,049	684
Earnings from continuing operations before income taxes	3,653	4,121	5,056
Provision for income taxes	1,204	1,427	1,741
Net earnings from continuing operations	2,449	2,694	3,315
Discontinued operations, net of tax	(4,085)	(723)	(316)

Net (loss)/earnings	$ (1,636)	$ 1,971	$ 2,999
Basic (loss)/earnings per share			
Continuing operations	$ 3.86	$ 4.24	$ 5.05
Discontinued operations	(6.44)	(1.14)	(0.48)
Net (loss)/earnings per share	$ (2.58)	$ 3.1	$ 4.57
Diluted (loss)/earnings per share			
Continuing operations	$ 3.83	$ 4.2	$ 5
Discontinued operations	(6.38)	(1.13)	(0.48)
Net (loss)/earnings per share	$ (2.56)	$ 3.07	$ 4.52
Weighted average common shares outstanding			
Basic	634.7	635.1	656.7
Dilutive effect of share-based awards	5.4	6.7	6.6
Diluted	640.1	641.8	663.3
Antidilutive shares	3.3	2.3	5

Table 2

Target's 2014 10Q Report

Expenses Incurred and Amounts Accrued

Data Breach Balance Sheet Rollforward (millions)	Liabilities	Insurance Receivable
Balance at February 1, 2014	$ 61	$ 44
Expenses incurred/insurance receivable recorded *(a)*	**26**	**8**
Payments made/cash received	**(35)**	**(13)**
Balance at May 3, 2014	**$ 52**	**$ 39**

Conclusion

After disclosure of SEC cybersecurity guidance, companies' disclosure on data breaches and cybersecurity has increased. There are studies on the interpretation the Guidance itself, but there are limited amounts of studies done regarding the effectiveness of the guidance. This literature review addresses the gap of the SEC cybersecurity guidance for further research questions. This literature review raises the concern of weakness of the disclosure. Further research is needed to address how companies react to the disclosure, which will bring more concern about cybersecurity guidance to SEC, investors and public companies' stakeholders.

References

Aguilar, L. (2014, June 10). Speech. Retrieved October 15, 2015, from http://www.sec.gov/News/Speech/Detail/Speech/1370542057946

Basic Incorporated v. Max L. Levinson, 485 U.S. 224 (Supreme Court. 1988)

Clark, M., & Harrell, C. E. (2013). Unlike chess, everyone must continue playing after a cyber-attack. Journal Of Investment Compliance (Emerald Group), 14(4), 5-12. doi:10.1108/JOIC-10-2013-0034

C, T. G., DePree, Chauncey M.,,Jr, & Grant, G. H. (2000). Earnings management and the abuse of materiality. Journal of Accountancy, 190(3), 41-44. Retrieved from http://search.proquest.com/docview/206786848?accountid=11667

Ferraro, M. F. (2014). "GROUNDBREAKING" OR BROKEN? AN ANALYSIS OF SEC CYBERSECURITY DISCLOSURE GUIDANCE, ITS EFFECTIVENESS, AND IMPLICATIONS. Albany Law Review, 77(2), 297-347.

Goolsby, A., Parks, R., & Sotto, L. (2011, October 19). SEC Issues Disclosure Guidance on Cybersecurity Matters and Cyber Incidents. Retrieved October 20, 2015, from https://www.hunton.com/files/News/a7719579-0584-464a-a78d-66cf46085ecd/Presentation/NewsAttachment/f9fcfbe7-bb41-4308-9fe8-66de4b157ec1/sec_issues_disclosure_guidance_on_cybersecurity.pdf

Gotshal, W. (2015, February 18). What's New in 2015: Cybersecurity, Financial Reporting and Disclosure Challenges. Retrieved September 18, 2015, from http://corpgov.law.harvard.edu/2015/02/18/whats-new-in-2015-cybersecurity-financial-reporting-and-disclosure-challenges/

Grant, G. T. (2014). SEC Cybersecurity Disclosure Guidance Is Quickly Becoming a Requirement. CPA Journal, 84(5), 69.

Lunn, Brad. (December 30, 2014). Strengthened Director Duties of Care for Cybersecurity Oversight: Evolving Expectations of Existing Legal Doctrine. Journal of Law and Cyberwarefare, 2014. Retrieved October 20, 2015, from http://ssrn.com/abstract=2544478

Park, M. (2015, March 19). Target Offers $10 Million Settlement In Data Breach Lawsuit. Retrieved September 16, 2015, from http://www.npr.org/sections/thetwo-way/2015/03/19/394039055/target-offers-10-million-settlement-in-data-breach-lawsuit

Rahm, S. (2014, November 1). Why investors should care about data security risk. Retrieved September 16, 2015, from http://www.schroders.com/staticfiles/Schroders/Sites/global/pdf/Why-investors-should-care-about-data-security-risk.pdf

SEC. (2011, October 13). CF Disclosure Guidance: Topic No. 2. Retrieved September 16, 2015, from https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

Stagliano, A. J., Sillup, George P. (2014, July). Transparency and Risk Assessment Reporting: A Case Study Sector Survey of Cybercrime Disclosures. Journal of Business and Economics, Vol. 5, No. 7, pp. 1134-1140, 2014. Retrieved October 19, 2015, from http://www.academicstar.us/UploadFile/Picture/2014-9/2014916102843567.pdf

Target-2015.01.31-10K. (2015, March 13). Retrieved September 12, 2015, from http://www.sec.gov/Archives/edgar/data/27419/000002741915000012/tgt-20150131x10k.htm

Trautman, Lawrence J. (November 5, 2012). Threats Escalate: Corporate Information Technology Governance Under Fire. Retrieved October 19, 2015, from http://ssrn.com/abstract=2171026

VORHIES, J. (2005, May 1). The New Importance of Materiality. Retrieved October 7, 2015, from http://www.journalofaccountancy.com/issues/2005/may/thenewimportanceofmateriality.html

Young, S. (2013). Contemplating Corporate Disclosure Obligations Arising from Cybersecurity Breaches. Journal Of Corporation Law, 38(3), 659-679