Accuracy of Self-Disclosed Cybersecurity Risks of Large US Banks

Troy G. Bakker
Dakota State University
ACCURACY OF SELF-DISCLOSED CYBERSECURITY RISKS OF LARGE US BANKS

By

Troy G. Bakker

DISSERTATION STUDY

Presented to the faculty of Graduate Studies and Research
Dakota State University
In partial fulfillment of the requirements
for the degree of Doctor of Science in Information Systems

Concentration: Information Assurance

Under the supervision of Dr. Kevin Streff

Madison, South Dakota

September 2015
We certify that we have read this project and that, in our opinion, it is satisfactory in scope and quality as a project for the degree of Doctor of Science in Information Systems.

Student Name: Troy Gene Bakker

Dissertation Title: Accuracy of Self-Disclosed Cybersecurity Risks of Large US Banks

Committee Chair: 

Date: 

Committee member: 

Date: 

Committee member: 

Date: 

Committee member: 

Date: 

Committee member: 

Date: 

Committee member: 

Date: 
ACKNOWLEDGMENT

I would like to thank my dissertation committee members; Dr. Streff, Dr. Figg, Dr. Peak, Dr. Podhradsky, and Dr. Sarnikar for all of their guidance in bringing this dissertation to fruition. I especially want to thank Dr. Streff and Dr. Sarnikar for helping me turn a very rough research idea into a full research project. Their assistance was invaluable.

I am also grateful for the assistance and support of my wife Victoria. Throughout my educational endeavors she has served the role of editor, sounding board, and sometimes unwitting test subject. She deserves as much credit for the completion of this degree as I do. She never gave up on me even when I had.
ABSTRACT

Since 2011, publicly traded corporations are required by the Securities and Exchange Commission (SEC) to self-disclose information security risks. However, because of several undefined factors, the risk information may not accurately reflect the threats within the Internet domain. Investors are then left ill-informed regarding this substantial risk to corporate value. This project quantifies the disparity between reported information security risks and information security threats finding that while reporting is becoming more accurate, corporations still only report 66% of cybersecurity threats they face.

This project also introduces a model that delineates factors that affect the accuracy of self-disclosed cybersecurity. The hypothesized factors are maturity, guidance, performance, and realization. Maturity is the number of years a company has been reporting cybersecurity risks, Guidance refers to the 2011 publication of a SEC document that instructs company’s on proper reporting methodology. Performance is the effect on a company’s profit or loss on accurate reporting and realization, the increase in reporting accuracy attributed to a company learning that they do face a particular threat.

Of the four factors analyzed in the model, only two were found to be relevant in determining cybersecurity risk reporting accuracy. Those two factors are maturity and guidance. Performance was not found to influence reporting accuracy. While there is anecdotal evidence to support the hypothesis that realization does improve reporting accuracy, there was not enough data on the report to corroborate this hypothesis.

The impact of this study is twofold, first if the maturation trend continues; reporting will improve to where they are reporting all of the risks that each corporation faces. The second
implication is that the SEC can control the accuracy of self-disclosed reports by instructing reporting institutions on how to prepare data for the reports they desire.
DECLARATION

I hereby certify that this project constitutes my own product, that where the language of others is set forth, quotation marks so indicate, and that appropriate credit is given where I have used the language, ideas, expressions or writings of another.

I declare that the project describes original work that has not previously been presented for the award of any other degree of any institution.

Signed,

[Signature]

Troy G. Bakker
# TABLE OF CONTENTS

**DISSERTATION APPROVAL FORM** ................................................................................................................ II  
**ACKNOWLEDGMENT** ................................................................................................................................ III  
**ABSTRACT** ................................................................................................................................................ IV  
**DECLARATION** .......................................................................................................................................... VI  
**TABLE OF CONTENTS** ............................................................................................................................... VII  
**LIST OF TABLES** ....................................................................................................................................... IX  
**LIST OF FIGURES** .................................................................................................................................. X  
**INTRODUCTION** ..................................................................................................................................... 1  
1.1 **BACKGROUND** ................................................................................................................................. 1  
1.2 **PROBLEM DEFINITION** ..................................................................................................................... 5  
1.3 **OBJECTIVES & APPROACH** ............................................................................................................... 9  
**LITERATURE REVIEW** ............................................................................................................................. 11  
2.1 **HISTORY OF SEC REPORTING** ........................................................................................................ 11  
2.2 **REGULATORY RISK REPORTING** ..................................................................................................... 32  
**RESEARCH METHODS** ........................................................................................................................... 36  
3.1 **OVERVIEW** ..................................................................................................................................... 36  
3.4 **SAMPLE SELECTION** ......................................................................................................................... 43  
3.5 **RISK CATEGORIES** ............................................................................................................................ 44  
3.6 **DATA COLLECTION** .......................................................................................................................... 47  
3.7 **DATA TRANSFORMATION** ............................................................................................................... 50  
3.8 **VALIDITY** ....................................................................................................................................... 52  
**RESULTS AND DISCUSSION** .................................................................................................................. 56  
4.1 **DATASET** ....................................................................................................................................... 56  
4.2 **DATA ANALYSIS** ............................................................................................................................... 59  
4.3 **COMPLETED MODEL** ......................................................................................................................... 74  
**CONCLUSIONS** ..................................................................................................................................... 76  
5.1 **FUTURE WORK** ................................................................................................................................. 77
# REFERENCES

APPENDIX A: ADDITIONAL DATA ANALYSIS

- Reported Risk by Type with Variance: ................................................. 85
- Risks by Entity ..................................................................................... 86
- Percentage Matching Risks by Entity .................................................. 87

APPENDIX B: GRAPHICAL OVERVIEW .................................................. 88

APPENDIX C: CODINGCATALOG ............................................................. 89

APPENDIX D: SCATTER DIAGRAMS ....................................................... 91

APPENDIX E: CF DISCLOSURE GUIDANCE NO. 2 ................................. 92

APPENDIX F: SEC ANTICDOTAL DATA .................................................. 97

- Google ............................................................................................... 97
- Amazon.com ....................................................................................... 98

APPENDIX G: SEC REGULATION S-K 229.503 (C) ................................. 100
## LIST OF TABLES

Table 1: Historical Response ............................................................................................ 12  
Table 2: Sample Entities ................................................................................................. 44  
Table 3: Risk Categories ................................................................................................. 46  
Table 4: Summation Risk Categories .............................................................................. 52  
Table 5: Summation of Risk .......................................................................................... 52  
Table 6: Coding Catalog Sample ................................................................................... 54  
Table 7: Dataset Sample ............................................................................................... 59  
Table 8: Hausman Test Output ...................................................................................... 60  
Table 9: Woodridge Autocorrelation ............................................................................ 61  
Table 10: Data Heteroskedasticity .............................................................................. 62  
Table 11: Cumulative Matching Percentage ................................................................ 64  
Table 12: Cumulative Matching Variance .................................................................... 65  
Table 13: Maturity Regression Values .......................................................................... 68  
Table 14: Performance Regression Values .................................................................... 69  
Table 15: Correlation Table ......................................................................................... 70  
Table 16: Guidance Regression Values ......................................................................... 72  
Table 17: Selected Entity 2011, 2012 DOS ................................................................. 73  
Table 18: Malware Reported after Target Breach ....................................................... 74
LIST OF FIGURES

Figure 1: Stock Price Disparity........................................................................................... 2
Figure 2: Risk Filters .......................................................................................................... 8
Figure 4: Federal Debt ...................................................................................................... 22
Figure 3: Research Model................................................................................................. 38
Figure 5: SEC Forms File ................................................................................................. 47
Figure 6: Selective FTP Script ........................................................................................ 48
Figure 7: Sample 10-K Hyperlinks ................................................................................... 49
Figure 8: Data Entry Application ...................................................................................... 51
Figure 9: Data Time Line ................................................................................................ 57
Figure 10: Heterogeneity Variable by Year ...................................................................... 61
Figure 11: Matched Threat Illustration ............................................................................. 62
Figure 12: Unmatched Threat Illustration ....................................................................... 63
Figure 13: Total Matching by Year .................................................................................. 66
Figure 14: Regression Analysis ........................................................................................ 67
Figure 15: Total Matching with Guidance ....................................................................... 71
Figure 16: Updated Model ............................................................................................... 75
Figure 17: Final Model ..................................................................................................... 75
INTRODUCTION

1.1 Background

Investors in corporate stocks and bonds rely on publicly available financial data collected by the Securities and Exchange Commission (SEC) to assist them with their investment decisions. The value of a corporation is of particular importance as an investor determines the price it is willing to pay for a share of a corporation’s stock. The value of a corporation is also affected by the risks that it faces. Risk indicates a threat to the earning potential of a corporation, which, in turn, affects the corporation’s value. An information security breach is one such threat to today’s information-centric corporations.

One does not have to look very far to see how an information security breach can affect a corporation’s value. The large international retailer, Target Corporation, was the victim of a massive information security breach in late 2013. The records of some 100 million customers were affected by the attack. The attack precipitated a nearly 50% drop in Target’s earnings for the fourth quarter of 2013. Ongoing costs are still unknown as litigation against the company due to the breach continues. Additionally, the retailer's stock lost approximately 9% of its value. Expenses associated with the breach in 2013 were more than 66 million dollars (McGrath, 2014).

Studies have indicated that stock price devaluation precipitated by a security breach is temporary in nature. Most stocks return to their previous level within a short amount of time, according to Acquisti, Friedman, and Telang (2006). This was true with the Target breach. Its stock price returned to its pre-breach level by November 2014. However, the Acquisti et al. study did not consider the stock price appreciation of competitors for the period. Walmart
Corporation, one of Target’s chief competitors, realized gains of 5 - 15% above Target’s appreciation. This disparity in stock price gains is demonstrated in Figure 1.

![Figure 1: Stock Price Disparity](image)

While Target has historically led Walmart in stock price appreciation, it was not until early 2015 that Target began to close the gap and lead again. This inequality in gains for 2014 indicated that Target’s stockholders were likely deprived of a stock price appreciation of $2 - 6 billion for most of 2014.

As indicated, the effect of the breach to shareholders was significant but they were unaware of the existing information security risk. The breach was the result of malware installed on Target's point of sale system (Constantin, 2014). However, Target's 2012 SEC-mandated risk report does not list malware as a risk. Furthermore, while Target does talk of the risk of a data breach it does not elaborate about the possible vector of a breach. Therefore, the investors were not informed that malware was a potential threat. Protecting the investing
public from this type of information deficiency is a major goal of the SEC. The Target example shows why the SEC has heightened its concern about information security risk issues.

The Target corporation breach is neither a new phenomenon nor an isolated incident. In fact, incidents are becoming more frequent and are costing companies more money (Aguilar, 2014). According to the SEC, cybersecurity incidents increased 42% from 2011 to 2012 (Aguilar, 2014). In a 2013 survey it was found that the financial cost of cybercrime had increased 78% from 2009 to 2012 (Aguilar, 2014). This escalation has not gone unnoticed by corporate directors. In a 2012 survey, 48% of corporate directors and 55% of corporate counsel viewed cyber security as their top concern (Corporate Directors, 2012).

The United States' securities markets have been touted as the most financially transparent in the world (Williams, 1999). This transparency is manifest in the accessibility of financial information available to investors (Williams, 1999) as well as its quality, which investors use to make informed decisions regarding the purchase and sale of investment vehicles such as stocks and bonds. The SEC-mandated information has a wide audience as more than 50% of US households invest directly or indirectly in corporate stocks and bonds (Saad, 2013).

While investor intent and knowledge may differ, one constant remains: they can all utilize the same publicly available financial information while making investment decisions. Availability of this information ensures that no group of investors has more or better information than the other. This symmetry of information availability and quality has been a goal of the SEC since its inception in 1933 (Williams, 1999).
Continuing its demand for accessible, high-quality data, in 2005 the SEC began requesting that corporations include material risk information on their mandated 10-K reports (SEC, 2005). In 2011, this request was altered to include information security risk data (Ferraro, 2013). The self-disclosed cybersecurity data communicates the risk that a corporation faces in day-to-day operation. The reported information is used by the investing public to help them determine if they are willing to invest in an organization with specific risks that may encumber corporate value.

As events similar to the Target breach affect more and more households, consumer visibility of such issues has also increases. This visibility prompted a group of legislators, led by Democratic Senator John Rockefeller, to notify the SEC that investors were not being properly informed of cybersecurity risks (Ferraro, 2013). This communication compelled the SEC to issue a guideline instructing corporations in how to complete the cybersecurity risk section of the 10-K report. The SEC hoped that additional guidance would increase the accuracy of the self-disclosed data.

However, this SEC guideline has been criticized as being vague and its effectiveness has been repeatedly questioned (Bronstein, 2012). The SEC has countered ineffectiveness claims with anecdotal data touting the successes of the guideline (Ferraro, 2013). While the subjective data appears encouraging, no analytical study has validated the SEC claims. This study is the first scientific study to examine the accuracy of cybersecurity risk reporting and factors that affect its accuracy.

It should be noted that the SEC was invited to participate in this study but declined; due to its policy against participating in academic research.
1.2 Problem Definition

The following two sections will deal with the definition of the problem that this thesis addresses. The problem statement will provide a brief statement of the problem and the problem history statement will go into greater detail regarding the history of the issue.

1.2.1 Problem Statement

Publicly traded corporations must supply the SEC with data regarding their information security risks. The data, which is included on the 10-K reports uploaded to the SEC’s online system, is used by investors to help determine the fair market value of a corporation’s stock. Unlike financial data, information security risk data is unaudited. This lack of oversight could allow for errors and misrepresentation of risk data. If the data is inaccurate, corporations may not be reporting all of the information security risk they face. These inaccuracies can result in an inflated stock price and a reduced understanding of the corporation’s true information security risks.

1.2.2 Problem History

Details regarding an organizations financial and operational performance are reported to the SEC on the mandatory 10-K report. That information is duplicated on the Annual Report that is sent to shareholders. Information from the 10-K report is also used to create a prospectus, which is sent to investors and potential investors.

Information contained in the 10-K report is not limited to financial data. Organizations are also required to include material corporate risks (Williams, 1999). The most commonly reported risks include government, competitive, business, and capital structure (Mirakur, 2011). In October 2011 the SEC released a communication giving corporations guidance about how to disclose information security risks on the 10-K report (Ferraro, 2013). By
publishing the guideline, the SEC has effectively informed organizations that it considers information security risk a material risk.

This increased concern of information security risk by the SEC is likely due to pressure on the agency by a group of senators led by John Rockefeller who want the SEC to be more influential in ensuring publicly traded corporations take the issue of cybersecurity risk seriously (Bronstein, 2012).

Although requiring the disclosure of cybersecurity risks on the 10-K report may appear to be innocuous, the implications are substantial. The SEC has effectively placed the responsibility for information security on top management for each publicly traded entity, insofar as it is top management that approves the data presented on the mandatory reporting. Additionally, the corporation’s stakeholders are made aware of potential information security risk through this mandatory reporting and thus no longer have plausible deniability.

This is an important change as information security within a corporation is often not understood by executive management (Katz & McIntosh, 2012). Furthermore, with the changes that the Sarbanes-Oxley act have facilitated, executive management may be personally liable if information security risk issues are not correctly reflected on the periodic reporting provided to the corporations stakeholders (Katz & McIntosh, 2012).

While 48% of corporate directors and 55% of corporate counsel viewed cyber security as their top concern (Corporate Directors, 2012), only one mandatory stockholder report addresses the issue and that is the 10-K report (for foreign companies, it is called the 20-F). This is a critical point and bears repeating: No other communication is required to provide information security risk information to a corporation’s shareholders. This exclusivity makes
the information security risk information on the 10-K report essential in determining the value of a corporation.

However, correctly reporting information security risk can be a difficult task for corporations because the guideline provided by the SEC is considered general in nature (Bronstein, 2012). The lack of detail leaves room for interpretation and interpretation could lead to inaccuracies. Furthermore, a corporation needs to balance risk disclosure while maintaining security. If it reveals a vulnerability to the public, it is at risk of inviting attacks (Bronstein, 2012).

Publishing a system flaw exposes the same issue Microsoft faces when they release patches for their products. When maintenance patches are released to correct a programming flaw, hackers reverse-engineer the patch to learn how to exploit the vulnerability. This presents a race situation between attackers taking advantage of a published vulnerability and computer users patching their systems. In fact, according to Microsoft’s manager of security and technology units, a system flaw has never been exploited before a patch was released (Ward, 2004). It is only after a patch the vulnerability is exploited.

As reported in a previous study, self-disclosed risk followed two paths before the SEC guidance. One path was to disclose risks an organization had already mitigated and the other was to disclose risk to avoid legal prosecution (Wang, Kannan & Ulmer, 2013). With the new SEC disclosure guidelines, organizations must disclose known information security risks regardless of the implications to the company. However, the new guidelines come after a long period of selectively disclosing risks to the public and investors. Therefore, it is possible that avoidance of disclosure has continued even after disclosure guidelines have been released.
The diagram below illustrates how corporate filters may affect the accuracy of information security risk.

![Diagram of risk filters](image)

Figure 2: Risk Filters

Because of corporate filters, investors should be concerned that they are not being correctly informed about the information security risk facing a corporation. While information security risk disclosure is mandatory, the SEC has given corporations very little instruction on how to report them. Therefore, the accuracy of information security risk reporting could be an issue and thus should be examined to determine if corporations are ignoring the weak SEC guideline and reporting inaccurate data to their investors.

The financial services industry is often a target of cybercriminals and therefore bears a large amount of information security risk (Crittenden, 2014). Not effectively responding to risks in this industry can be very costly to an investor and, in fact to the as demonstrated by historic banking crises throughout the years and most recently the 2007 - 2008 crisis. Therefore, determining the accuracy of information security risk reporting by the banking industry is important to investors, banking regulators, and the world economy.

This effect is obvious when reviewing the consequences of banking misadventures. Recent mishaps include the increased failure of savings and loan banks in the early 1980s and more recently the subprime lending debacle in the late 2000s. Each of these incidents had a long term negative effect on the economy.

It is because of this high concentration of risk that the scope of this dissertation is the banking industry. Banking is a highly regulated business sector. The regulating authorities
include the Comptroller of Currency, the Federal Reserve System, Federal Deposit Insurance Corporations, and finally the various state regulatory commissions (Hutchinson, 1988). If the bank’s stock is publicly traded, then the Securities and Exchange Commission is also involved.

Although the number of agencies regulating banking institutions may appear excessive, improper management of a financial institution can have a profound effect on national or world economies.

1.3 Objectives & Approach

Along with determining if risk reporting is accurate, this project presents and evaluates a model that hypothesizes the determining factors in the accuracy of information security risk reporting. The factors that are hypothesized to affect the accuracy of risk reporting are presented below;

1. Lack of guidance as to how to report cybersecurity risk (guidance)
2. Inexperience in determining the appropriate cybersecurity risk to the corporation (maturity)
3. Intentionally underreporting in light of bad financial results (performance)
4. Not realizing a particular threat is present in the industry (realization)

These factors guidance, maturity, performance, and realization constitute the independent variables in this analysis of risk reporting accuracy.

The first task in this analysis is the quantification of reported information security risks inaccuracies. This was accomplished by taking a sample of publicly traded corporate banks’ self-disclosed information security risk data and comparing that data with known
threat data. The threat data was obtained inductively by reviewing the sample banks reported information security risks reports and categorizing the risks into general threat categories. The threat categories were then reviewed and distilled into 12 general categories. These twelve categories were identified as industry threats.

Differences between industry threats and self-disclosed risk revealed inaccuracies in the self-disclosure process. To determine the level of inaccuracy industry, threats were compared to self-disclosed risks over several years. The level of disparity between reported risks and threats fluctuated throughout the years as events related to the hypothesized factors occurred. Analyzing this disparity allowed for quantification of the hypothesized independent variables for the proposed model.
LITERATURE REVIEW

This study examined reported self-disclosed cybersecurity risk qualitative data collected by the SEC. Unlike financial data provided to the shareholders, cybersecurity risk is unaudited (IAS Plus, 2014). The shareholder must therefore rely on the reporting corporation to ensure that the data is correct. This study will determine if cybersecurity risk data reported by large US banks is in step with cybersecurity threats. To that end, this literature review will examine the following information, which is available in the knowledge base of the information assurance domain.

- Brief history of SEC reporting
- Similar studies using Regulatory Risk Reporting

2.1 History of SEC reporting

The SEC has mandated that publicly traded corporations provide specific data regarding the financial health and operations of a regulated corporation. The type of mandatory reporting required by the SEC has changed over the 81 years that the SEC has been in operation. However, considering the complicated nature of financial reporting, changes have been scarce. The major changes to SEC requirements have followed significant instability within the markets (Federal Securities Laws) as indicated in Table 1:
Table 1: Historical Response

<table>
<thead>
<tr>
<th>Market Event</th>
<th>SEC Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stock market crash of 1929</td>
<td>Securities Act of 1933</td>
</tr>
<tr>
<td></td>
<td>Exchange Act of 1934</td>
</tr>
<tr>
<td>Advisors not adequately informing customers regarding risk in investment</td>
<td>Investment Advisers Act of 1940</td>
</tr>
<tr>
<td>Investment</td>
<td></td>
</tr>
<tr>
<td>The great recession 2007 - 2008</td>
<td>Dodd-Frank 2010</td>
</tr>
<tr>
<td>Sluggish growth as Economy recovers from the Great Recession</td>
<td>Jumpstart our Businesses Act - 2012</td>
</tr>
</tbody>
</table>

The events and SEC response to the events can be looked at in different ways. One way is that SEC is working to correct the egregious activities that threaten to destabilize the U.S. economy. The other way is that the event-and-response approach of the SEC can be interpreted as a lack of foresight by the SEC and the elected policy makers.

2.1.1 Blue Sky Legislation

Before the SEC was created by the Securities Act of 1933, securities transactions were governed by “Blue Sky” laws. The legislation that created the Blue Sky laws was enacted at the state level; they are not federal law (Macey, 1991). The first state to enact the laws was Kansas in 1911. The laws became necessary toward the end of the 19th century, the stock and
bond markets were becoming more accessible. Previously, stock and bond investors were wealthy, experienced business persons, or corporations. This was changing rapidly as middle class incomes rose and inexperienced investors entered the markets (Macey, 1991).

The make-up of securities in the stock and bond markets was also changing. They began to include more speculative offerings to the public. While experienced investors were aware of the risks involved with speculative securities, new investors were not. There were also offerings that were simply fraudulent, taking advantage of the influx of inexperienced investors (Macey, 1991).

Unscrupulous securities promoters used aggressive advertising campaigns to promote high-risk investment opportunities. The campaigns played on the greed and inexperience of the new investors. It was within this environment that market regulation was born. The Blue Sky laws were enacted to protect investors from fraudulent claims, not to curtail speculative investment (Macey, 1991).

The Blue Sky laws required firms that wished to sell securities within the state where the laws had been enacted, to obtain a license from the bank commissioner. The entity selling the security was also required to provide periodic reports detailing the financial condition of the entity for which they were selling stock. Legitimate investment bankers opposed the legislation. They opposed it not because it would eliminate fraudulent security sales but because the same rules would apply to them. The legislation would also increase the cost of selling securities. Also, the legitimate investment bankers were trying to distance themselves from the fraudulent or highly speculative firms selling investments. Being forced to adhere to the same regulation as an unestablished company may have been somewhat insulting (Macey, 1991).
Shortly after Kansas adopted the legislation, many other states enacted the Blue Sky laws or similar legislation. States that did not have an active investment banking market were more likely to adopt Blue Sky legislation (Macey, 1991). This is likely due to the lobbying of legitimate investment bankers attempting to avoid the added overhead that would follow the legislation.

Some have argued that in the early 1900s fraudulent stock offerings were very rare. It was the promotion and sale of highly speculative offerings that was the impetus of the Blue Sky laws not runaway fraud and corruption (Macey, 1991). Even with the creation of the SEC, Blue Sky legislation remains in many states. The laws are used when dealing with the legality of the sale of securities at the state level.

2.1.2 Creation of the SEC

In the early 20th century the prevailing attitude toward business regulation was that of laissez-faire. It was assumed that supply and demand would allow business to be self-regulating. Before the market crash of 1929 the U.S. economy was strong and growing rapidly (Keller, 1988). The Gross National Product grew at an annual rate of 4.7% from 1922 to 1929. The unemployment rate was a very low 3.7% (White, 1990). The stock and bond markets were strong - likely being bolstered by novice investors. These inexperienced investors began entering the markets as the income of the middle class rose. They also drove up stock prices as they were deficient in evaluating the true worth of a stock (White, 1990). It looked to policy makers that all was going well and there was no reason to impose regulation on banks or any other industry.

Because of the inflated stock prices, businesses found that they could avoid large bank loans by issuing equities. With corporate borrowing slowing, credit was easily available and
inexpensive, which allowed investors to purchase stock on margin (Bhide, 1991). On October 24, 1929 known as Black Thursday and October 29 Black Friday, stock prices plummeted. The drop in stock value initiated margin calls and panic selling. Stocks listed on the New York Stock Exchange would continue to fall and lose 83% of their value. The market would not recover to pre-crash levels until the mid-1950s (Bhide, 1991).

It was in the wake of this near financial collapse that congress enacted the Securities Act in 1933. The Exchange Act was approved by Congress in 1934. The federal laws mandated by the Securities Act and the Exchange Act borrowed heavily from the Blue Sky legislation (Macey, 1991). Borrowing from previous legislation was a prudent practice as the Blue Sky legislation had been in place for more than 20 years and had been altered throughout the years to rectify issues that were discovered after the legislation was put into place (Macey, 1991). This provided a template in which to model the new Federal laws.

Even today we can still see similarities in the federal laws dealing with publicly traded companies and the Blue Sky laws (Macey, 1991). Both the Blue Sky laws and the current laws emphasize accurate reporting of the financial condition of a business before stock can be sold. The laws also require that the financial information be reviewed and approved by an authorized party. The authorized party has the authority to deny the applicant the ability to sell stock for an entity that does not meet the established standards.

The new laws enacted with the creation of the SEC were an attempt to protect investors and ensure that all investors have the same information available to them. The following is a summary of efforts by the SEC (Bhide, 1991):

1. Publicly traded securities must register with the SEC. Registration included information regarding the financial condition of the organization. Registrants were
also required to provide information regarding the company's directors and major investors

2. Registrants were also required to provide updated financial and governance information on a quarterly and yearly basis.

3. The use of proxy voting is scrutinized to ensure that stockholders are aware of the issues for which their vote may be used.

4. Criminal penalties were established for willfully misrepresenting information regarding the condition of the corporation to its shareholders.

5. The SEC was also given the ability to withdraw a company's registration to sell securities if they did not adhere to the reporting requirements.

6. Material trading actions by the corporation’s directors was made available to all shareholders.

2.1.3 New Banking Regulation

Banks, especially small rural banks struggled during the Great Depression. Bank failures were commonplace. With 30,000 banks in the United States, 9,000 banks failed or suspended service (Wheelock, 1995). In 1932 Congress, with encouragement from the Roosevelt administration, called for a banking holiday. During this holiday all banks were shut down. Only banks that had the approval of the regulators were allowed to reopen after the holiday (Wheelock, 1995). Much has been written regarding the effect bank failures had on the longevity of the Great Depression but there is little consensus. However, the creation of the Federal Deposit Insurance Corporation that guaranteed deposits against bank failures is credited with restoring public confidence in the 1930s banking system (Wheelock, 1995).
To eliminate issues that were perceived as deficiencies of the U.S. banking system, the Glass-Steagall Act was passed in 1933. The focus of this legislation was to separate commercial banks from investment and trust banking activities. The intent of this separation was to ensure there was no conflict of interest as the banking organizations performed their fiduciary duty for trusts (Bhide, 1991). An example of conflict of interest is when banks offer investment products to customers, and steer their customers to a product with higher fees but more risk. Another example is when a banker notices a large balance in a savings account and recommends the account hold put the money into the stock market. While this may be a good investment option for both the bank and the investor, the investment is more speculative and the investor bears more risk.

Another conflict of interest can occur between the investment bank and the commercial lender. The commercial bank may have a customer that has defaulted or will default on a loan; however, the bank can prevent that default by issuing securities. The investment bank operation sells the shares they then use those capital funds to pay the commercial loan. This allows the bank to avoid losing money if the customer defaults. The stockholder is then left with stock that has little or no value (Bhide, 1991).

It is unclear to what extent this type of activity occurred. However, as the issue was debated, the public was appalled by the possibility of being deceived by their banks. They supported the legislation for separating the banking functions. However, only banks that were members of the Federal Reserve System were affected by the legislation. Non-member state banks were not bound by the Glass-Steagall legislation (Hutchinson, 1988).

The idea of restricting banks activity was more about political posturing than a practical deterrent to protect consumers (Hutchinson, 1988). The Glass-Steagall Act was
effectively repealed by the adoption of Gramm-Leach-Bliley Act in 1999. Commercial Federal Reserve member banks were once again allowed to act as a brokerage house.

### 2.1.4 Sarbanes-Oxley Act

The Sarbanes-Oxley Act was passed by congress in 2002. This legislation was enacted as the deceptive accounting practices of several corporations’ were brought to light. The publicized corporations that were employing deceptive accounting practices included Enron, World Com, and Tyco (Ge & McVay, 2005).

The intent of the legislation is to ensure that executive management of a publicly traded company is accountable for the financial information that is being provided to investors and regulatory agencies (Ge & McVay, 2005). The legislation states that it is the responsibility of executive management to assess the internal control mechanisms enacted by a corporation. Information regarding internal controls is new for SEC reporting. The only other reporting vehicle that requires assessment of internal controls is the Foreign Corrupt Practices Act (FCPA) implemented in 1977. Many corporations do not have dealings with foreign countries so they are exempt from publishing the report. Therefore, for many corporations, internal controls exposure mandated by Sarbanes-Oxley was the first time corporations were required to review the company’s internal controls (Ge & McVay, 2005).

Substantial criminal penalties can be imposed upon a corporation’s management if it intentionally approves a false reporting vehicle that is presented to investors or regulating entities. The penalties can be a fine of up to $5,000,000 and a maximum of 20 years in prison (Ge & McVay, 2005). The severity of sanctions for falsifying reports is an indicator of how important accurately communicating a corporation’s financial condition is to the public.
2.1.5 Banking Crisis of 2007

Although the 2007 banking crisis had little to do with the SEC’s regulation of corporate stock, it is a fine example of how the lack of regulation can go awry. According to the Office of the Comptroller of Currency (OCC), national banks are among the most highly regulated industries in the United States (Laws & Regulations, n.d). Even with this high degree of reporting and evaluation, unexpected issues can arise that require foresight and understanding of the banking industry. Without this understanding and prudence, issues such as the banking crisis of 2007 are inevitable.

The 2007 banking crisis also serves as a reminder of how integrated banking is to the everyday process of practicing business in an industrialized country. Not only is the integration of banking and business limited to domestic endeavors, banking issues in the United States can also affect businesses and economies internationally. It is for these reasons that the SEC and other regulators keep a close eye on the U.S. banking system.

The banking crisis that occurred during the Great Depression was not the first incident of this kind. In fact, the U.S. has experienced banking crises of varying severity in 1857, 1893, 1907, 1929, 1981, and most recently 2007 (Bordo, 2008). However, the financial crisis of 2007 has been touted as the worst economic downturn since the Great Depression. The severity of the recession of 2007 has led many to coin the crisis as the Great Recession (Bordo, 2008).

Although there are different theories as to the cause of the Great Recession few argue against the subprime mortgages as a major contributor. The subprime bubble was created during a period of historically low interest rates. The interest rates were low as result of the Federal Reserve’s loose monetary policies between 2001 and 2004 (Bordo, 2008). Subprime
mortgages are mortgages granted to individuals that are a higher risk for default. Another player in the subprime mortgage market is the shadow banking system. The shadow banking system is a collection of nonbank financial intermediaries. The creation of the shadow banking system was made possible by the repeal of the Glass Steagall Act in 1999 (Bordo, 2008).

Shadow banking entities are operated outside the jurisdiction of the Federal Reserve Banking System. Also, the capital requirements of the shadow banking system are lower than that of commercial banks. Lower capital requirements mean they carry more risk (Bordo, 2008). As interest rates began to rise in the years before the crisis, the subprime borrowers with adjustable rate mortgages saw their payments jump. Since many of the lenders overextended their financial position by purchasing a subprime loan, the effects of an increased mortgage payment put many lenders in a position where they could no longer afford their mortgage payments. This, in turn, resulted in the default of their mortgage loan.

Although the financial industry had expected a higher default rate for subprime loans, they expected that property values would continue to rise. With the inflated property values they would be able to recoup their losses from the sale of the foreclosed property. However, because of the volume of defaulted loans and the poor capitalization of the banking and shadow banking systems, property values began to decline. This caused the United States’ financial markets to be thrown into a crisis situation.

Events that exacerbated the 2007 banking crisis happened very quickly. One of the most profound events of the crisis was the failure of the investment bank Lehman Brothers. Other large entities were also on the verge of failure. This brought up a new term in the financial markets - “too big to fail” (Mishkin, 2010). This concept meant that some
organizations were so interconnected within the financial markets that their failure would be catastrophic to the financial markets (Bordo, 2008). This prompted the United States government to assist several large corporations in their struggle to maintain solvency. Some of the corporations that benefited by being interconnected were AIG, Bears Sterns, and government sponsored enterprises such as Fanny Mae, and Freddy MAC (Bordo, 2008).

As the crisis worsened and commercial banks struggled to maintain safe levels of capitalization, corporate lending was severely restricted (Bordo, 2008). In an attempt to alleviate the liquidity issues that banks were facing, the U.S. Treasury began the Troubled Asset Relief Plan (TARP). Although TARP funds were originally intended to purchase mortgage backed securities, it was transformed into a method of injecting capital into the banking system (Miskin, 2010). The TARP program injected 700 billion dollars into the banking system as it purchased non-voting shares in the largest banks in the United States (Bordo, 2008).

Not all the banks that received TARP funds were grateful for the emergency funds. The CEO of Wells Fargo, Dick Kovacevich insisted that Wells Fargo did not need the infusion of capital and Wells Fargo was basically forced to take the TARP funds (Belveder, 2013). Such banks found themselves accountable not only to the shareholders of the bank but to the U.S. government and taxpayers. Entities that were provided a government “bail out” during the financial crisis found themselves under scrutiny especially regarding sensitive issues, such as executive compensation and perks.

Although the financial crisis of 2007 is over and the majority of the TARP funds returned to the treasury, could this crisis have been avoided with proper regulation in place? The financial institutions as well as government regulators were aware of the growing use of
subprime lending in the United States. Banks were also aware of the risky nature of subprime lending. Financial institutions that believed subprime lending was too risky to participate in lending, were at an earnings disadvantage for many years as their completion embraced subprime lending despite the risks. Only after the bubble had burst were the risk takers called to account for their actions.

The subprime bubble raised the U.S. debt to more than 100% of the GDP, a level that has not been experienced since the end of World War II (Chantrill, n.d.). As indicated in Figure 4: Federal Debt, the U.S. taxpayer is paying dearly for the lack of oversight by our elected officials.

![Federal Debt](image)

**Figure 3: Federal Debt**

### 2.1.5 New regulation following banking crisis of 2007

As what appears to be the norm, the banking crisis spurred legislators to develop new laws to prevent the incident from being repeated. The legislation passed during the 2007 banking crisis is called the Dodd Frank Act. Although the Dodd Frank Act is a long and
detailed piece of legislation, it has only two objectives. The objectives are to address and curtail the risks associated with the shadow banking system and minimize the risks inherent with those entities that were considered “too big to fail” (Skeel, D. 2010).

Congress's approval of the Dodd Frank Act was assisted by a lawsuit levied against a large brokerage company named Goldman Sachs. The legal proceedings alleged that Goldman Sachs had sold mortgage-backed securities for mortgages that were expected to fail. This information was not passed onto the purchaser of the investment thus prompting the lawsuit (Skeel, D. 2010). The public was outraged by the implications of the lawsuit and backed the increased regulation put forth by the Dodd Frank Act.

To accomplish the objectives of the Dodd Frank Act, regulation needed to be expanded to include those of the shadow banking system. The act required that derivative agreements between companies be done so one an exchange (Skeel, D. 2010). This prevents a company from having off-balance sheet liabilities that remain unreported. The other goal of Dodd Frank is accomplished by identifying those institutions that could cause a cascading affect through the financial system if they failed (Skeel, D. 2010). The major collection of these institutions were defined as “too big to fail” during the crisis of 2007. According to the Dodd Fran Act, institutions that are “too big to fail” are subjected to increased monitoring and required to maintain higher levels of capitalization.

2.1.6 Lessons Learned – Great Depression & 2007 Banking Crisis

If there is a lesson to be learned regarding the transparency of financial institutions it is that regulatory bodies need to be vigilant in monitoring the financial system of the United States. Monitoring and reporting for these critical financial players need to change as the financial industry changes. The risks that a company faced 20 or even 5 years ago may change
drastically in today’s market. This lack of transparency and unregulated risk in the 2007 economy is evident when the major regulators were unaware of the delicate financial condition of Bear Stearns investment bank and other institutions (Skeel, D. 2010).

The response to risks made apparent by the Great Depression saw the creation of the Federal Depositors Insurance Corporation and the SEC. The 2007 banking crisis saw the creation of the Financial Stability Oversight Council and the Consumer Financial Protection Bureau (Skeel, 2010). It is apparent from historical events that the regulation of risk in the financial markets is reactionary and not a system that is engaged in evaluating potential risks to protect the public from currently unseen risks.

The requirement and the encouragement by the SEC for publicly traded entities to reveal potential cybersecurity risk is therefore an aberrant event - aberrant if we assume there has not been a crisis; par for the course if we assume that an information security crisis has already taken place.

2.1.7 Cybersecurity Crisis in banking

Is there a cybersecurity crisis in the banking industry? The term cybersecurity was first used in the 1990s (Hansen & Nissenbaum, 2009). The issues related to the security of devices connected by a network have changed significantly from the 1990s. Today, cybersecurity deals with issues that are extremely serious in nature. The SEC in the 2011 CF Disclosure Guidance Topic Number 2 refers to cybersecurity as "the body of technologies, processes and practices designed to protect networks, systems, computers, programs and data from attack, damage or unauthorized access"

As the networking of everyday actives increases, so does the importance to secure the activities. The security of a household banking assets is of primary importance, thus bringing
the issue of cybersecurity in banking immediately to the forefront of concern. However, does this indicate a crisis?

Securing banking transactions from those who attempt to steal has been a race of technology. The use of safes and locks pitted against gunmen and explosives, secure checking against forgery and fraud, secure accounts, passwords and protocols against hackers and crackers. This race has been evident in the many incidents reported by financial institutions as they attempt to stay one step ahead.

Some of the most egregious examples of data security breach include the 2008 breach of Heartland payment systems where a SQL Injection Attack exposed the credit card details of 134 million customers and the 2007 TJX network attack, which exposed the credit card information of 94 million customers (Armerding, 2012). More recently is the Target Corporation’s exposure of more than 100 million customers’ credit and debit card information in a point of sale exploitation during a busy shopping season (Hughlett, Ramstad & Crosby, 2014).

Although none of these examples was directly due to a security deficiency in the banking industry, all affected the financial vehicles of the industry and perhaps the industry’s reputation. Studies have shown that corporations that experience a data security breach suffer a short-term negative effect in stock price (Campbell et al., 2003; Acquisti et al., 2006). While, quantifying the effect on a corporation’s reputation is a more difficult, the impact is likely longer lasting.

Although extending banking operations to the Internet domain opens a banking institution to more risk, they are often forced to take the risk by the simple mechanism of competition (Munirul, Zuraini & Sailani, 2011). As more banks offer Internet banking, other
bonds are forced to enter into this market even if they are not operationally and procedurally ready for such a venture.

Poor information security performance can dissuade customers from choosing a specific bank for their Internet banking needs (Munirul, Zuraini & Sailani, 2011). Therefore, applying good information security principles as a normal part of bank operations is important to the financial wellbeing of a bank. Furthermore, capitalization requirements for a banking entity are affected by the amount of risk the bank holds. If a bank carries a large amount of risk, they must hold an increased amount of money in reserve to meet capitalization requirements set forth by banking regulators (Calder & Watkins, 2010). This capital is held on the balance sheet as a nonperforming asset, meaning the bank loses money on the balance it needs to hold in reserve. Therefore, the higher a reserve, the less money the bank has to loan or invest.

Several organizations have brought forth information security standards that a bank can employ to deal with information security issues. Some such standards include ISO 27002, COBIT, FFIEC, etc. (Munirul, Zuraini & Sailani, 2011). Adopting and complying with such a standard can help ensure that a bank is ready for the added risk of doing banking within the Internet domain. However, each of these standards has strengths and weaknesses thus requiring a bank to customize portions of the standard to their particular business practices (Munirul, Zuraini & Sailani, 2011). Mixing and matching aspects of these standards can cause confusion as a bank may not comply completely with one specific standard. The confusion may be on the part of the bank its customers or regulating authorities. It is only through a professional evaluation of a specific banks security framework that one can truly understand if a bank has an adequate level of information security (Munirul, Zuraini & Sailani, 2011).
Adding to the confusion in complying with a security standard, is the requirement to adhere to new legislation affecting banks after the 2007 financial crisis. While large banks generally have the resources to deal with the increase in government oversight, smaller banks may suffer with compliance as they are forced to wade through the new requirements (Derek, 2015). This can become a difficult task as smaller banks do not necessarily have the staff or expertise to deal with the compliance issues (Derek, 2015). Furthermore, staffing of cybersecurity professionals may not only affect small banks. There is a lack of properly trained cybersecurity professionals in the work force today (Evans & Reeder, 2010).

While we have not seen egregious examples of a cybersecurity crisis in the banking industry, the elements for a crisis exist. Banks are offering products with little understanding of how those products may increase their risk. The standards they attempt to adhere to may not be sufficient and regulators may not catch a banks unmitigated risk due to information security until there has been an issue. Therefore, a cybersecurity crisis in banking may be on the horizon as banks continue to struggle with issues related to securing their data and transactions.

2.1.8 Disclosure Topic Number 2 - Cybersecurity

The SEC began communicating its desire for more cybersecurity risk disclosure to public corporations in October of 2011. The communiqué was issued without legislative ruling. Because it was not followed up with legislation, corporations are not bound to this new requirement (Ferrao, 2013). However, the SEC is proceeding as if the requirement is law. The name of the communiqué is Disclosure Topic Number 2 - Cybersecurity (CF DG 2). The disclosure claims authority from the Securities and Exchange Acts of 1933 and 1934. As previously discussed, the intent of the legislation was to ensure that public corporations reveal
material risks to their investors. As evident by the concern of the public and corporation executive management (Katz & McIntosh, 2012), cybersecurity has become an issue that needs to be addressed.

Because the goal of the communication affects the private sector, there have been questions regarding the legality of the disclosure requirement. The issues related to the legality of Disclosure Topic Number 2 - Cybersecurity is beyond the scope of this paper.

In June of 2011 the Senior Deputy Controller of the Office of the Comptroller of Currency (OCC) released an OCC bulletin to financial institutions. The purpose was to remind financial institutions of a communication sent in 2005 (Long, 2011). The original communication reminded banks of their obligation to secure on-line banking accounts. The document also released a guideline as how banks should instigate controls within their entity. The 2011 document informed financial institutions, primarily national banks that they would have to conform to the guidelines presented to the banks in 2005. Furthermore, the institutions were audited beginning in January 2012 to ensure appropriate controls are in place.

Although the OCCs risk control guidance document is vague and directed toward online accounts, the message was much the same as the CF DG 2. Banks need to ensure that controls are in place to prevent cybersecurity issues. The appropriate section of the CF DG 2 document has been attached as Appendix E.

Furthermore, Senator John Rockefeller raised the exposure of the communiqué' by expressing his approval of the measure to then SEC chairperson, Mary Shapiro. The communication between the senator and the SEC occurred in April 2013. Senator Rockefeller also requested that the effort be given more attention insofar as corporations need to take cybersecurity risks seriously (Young, 2013). Lack of attention to this issue could put the
investor at a disadvantage by not being informed of material risks of the corporation in which it has invested. The senator previously expressed his concerns to the SEC in May of 2011. The October communication was likely a response to the senators written concern.

Rockefeller's efforts in 2011 and 2013 were not those of a single senator’s crusade as several Democratic senators added their names to the letter sent to the SEC (Young, 2013). It is possible that the letter was a precursor to political posturing for adding SEC regulation to the failed Critical Infrastructure Act. The SEC chairperson promised she would review the disclosure requirements (Ferrao, 2013). The June 2011 communication from the OCC is also likely a response to the growing concern expressed by Congress and the public in general.

Responding to Rockefeller's 2013 request for greater exposure of cybersecurity risk disclosure by the SEC, Chairperson Shapiro responded citing the sufficiency of the October 2011 communication (Ferrao, 2013). Shapiro demonstrated the supposed adequacy of the communication by revealing fifty case studies of companies that had already been informed of their deficiency in disclosure (Ferrao, 2013). Two of the case studies have been critically examined by the *Albany Law Review* (see Appendix F).

The *Albany law review* has determined that the October 11 communication is not an effective disclosure vehicle nor does it have the authority to enforce accurate disclosure. The opinion was established as the cases were reviewed for disclosure actions taken after the SEC expressed concern regarding disclosure of known issues (Ferrao, 2013). Indifferent to the opinion of the *Albany Law Review*, as of January 2014, the guideline has not been usurped by a more extensive policy.
2.1.9 SEC Guidance Instructions

The SEC’s October 11 guidance document will be called CF DG 2. This is short for Corporate Finance Disclosure Guidance Topic Number 2. CF DG 2 appears in regular SEC communications and is maintained on the SECs website. The document is fairly short and outlines the following points;

1. Digital communication has been ever increasing.

2. Cybersecurity issues have increased.

3. The guidance has been prepared to ensure that publicly traded corporations are in compliance with SEC disclosure laws stated by the SEC Acts in 1933 and 1944.

4. Material risks need to be reported on the 10-Q and 10-K reports.

5. There are no other federal laws that require the collection and publication of cybersecurity risks.

6. The company must determine the materiality of a risk of incident and report that incident. The company should also include information regarding the costs and issues related to a cybersecurity.

7. Material events need to be reported on report 8-K. Section 8 refers to other material events. This may logically include cybersecurity events (Young, 2013).

8. Disclosure of a cybersecurity issue that may have been undetected for a length of time.

9. Disclosure should be specifically related to the risks determined by the company. The company should avoid "Boiler Plate" rhetoric as they discuss cybersecurity risk.

10. The language of the 10-Qs.55 and 10-K reports should be straight forward and easy to comprehend.
11. Not only should cybersecurity issues be disclosed, the immediate and ongoing losses should be disclosed.

12. Legal proceedings resulting from cybersecurity incidents need to be disclosed.

13. The company should have controls in place to deal with cybersecurity issue disclosure.

2.1.10 Preparation of 10-K & 10-Q

The instructions for completing the required disclosure are included with the 10-Q and 10-K instructions (10-Q is a quarterly report). From this point on, this paper will discuss the 10-K report. These instructions are available on the SECs main website. The risk section for the 10-K report is Item 1A, Risk Factors. The instructions refer the filer to risk factors described in item 503(c) of regulation S-K 229.503 (c). The document has been included in Appendix G.

As evident in Appendix G, the preparation instructions for risk disclosure are extremely general in nature. There is no defined methodology or even a systemic approach to the mechanics of completing the report. In fact, the CF DG 2 document, while vague, has more concrete instruction than the formal instructions for the risk section of the 10-K report. Because the instructions do not provide a formal format, the resulting reports are unique to each entity. Therefore, it can be very difficult for an investor, or a researcher, to extract important data from the report. This can be of concern because this is the only place where a publicly traded corporation is asked to disclose information security risk.

2.1.11 Preparation 8-K

Although, not included in the CF DG 2, normal SEC disclosure reporting includes the preparation of form 8-K. This form is for reporting material events during the forms indicated
period. Section 8 of the form has a section for “other events”. The instructions require that corporation include events that would be of interest to the stockholders. It has been argued that cybersecurity breaches should be included as a material event in this section of the self-disclosed events (Young, 2013).

In 2004 the SEC changed the requirements for form 8-K to include a wider variety of events. It also expedited the reporting of the event to 4 days. Some had speculated that this increased interest in form 8-K would reduce the amount and quality of meaningful information presented on the 10-K and 10-Qs reports. Lerman and Livnat investigated this concern by reviewing the 8-K, 10-K and 10-Qs reports for over a half million filings. Their findings indicated that information on the 10-K and 10-Qs reports was not reduced in volume or value (Lerman & Livnat, 2009).

2.2 Regulatory Risk Reporting

With the scarcity of like projects, this study will examine closely related ventures with the hopes of drawing a parallel with other studies on self-disclosed risk. Although the SEC requested cybersecurity risk data in 2011, they previously required corporations to disclose other types of material risks on their mandatory reports (Helbok & Wagner, 2006). The most commonly reported risks are related to capital, competition, personnel, government, and economic environment (Mirakur, 2011). Scientific studies have been performed on some of this risk data and will provide the parallel needed for the literature review.

The first such study was researching operational risk (OR) reporting. Although the SEC did not require OR reporting in 1998, researchers found that the disclosure of OR between 1998 and 2005 was significant and was showing signs of maturity (Helbok &
Wagner, 2006). Value at Risk (VAR) is an indicator of the risk in a bank's portfolio. In 1998, the SEC mandated that banks begin reporting (VAR). By 2001, the VAR indicator was added to nearly all regulated bank's 10-K reports (Jorion, 2002).

Independent analysis of VAR in 2002 indicated that the self-reported VAR is accurate and useful to the shareholder. Furthermore, it appears that the reliability of this index is maturing as banks learn more about the preparation of VAR (Jorion, 2002). In a later study, qualitative risk data was collected from corporations between 2005 and 2008. Researchers analyzed the data and determined that the risks presented on the 10-K reports were accurate (Campbell, Chen, Dhaliwal, Lu & Steele, 2011).

Researchers also discovered that shareholders were reacting to the reported risk data (Campbell, Chen, Dhaliwal, Lu & Steele, 2011). The shareholder’s reaction resulted in the increased value of a corporation when risk factors were low (stock prices rose). The converse was also true. When risk factors were high, stock prices fell (Campbell, Chen, Dhaliwal, Lu & Steele, 2011). This indicates that shareholders do react to risks presented in the 10-K report.

In a 2009 Dutch study, researchers analyzed the prospectus information sent to shareholders to determine if they were being properly informed of corporate risk. The risk portion of a prospectus is not materially different from the 10-K report. In this study they found that the risk statements were an adequate indicator of future risks (Deumes, 2008).

Other studies have utilized self-disclosed cybersecurity risk as an indicator of a potential data breach (Wang, Kannan & Ulmer, 2013) or perception of risk (Campbell, Chen, Dhaliwal, Lu & Steele, 2011) but none compared the data to the reported threats. Furthermore, previous studies have not been conducted using data collected after the 2011 SEC guideline was published. One of the first studies that focused on the “1A Risks” section
of the report was a 2011 study by Campbell et al. This study classified all risks grouping information security risks into general categories and once again discovering that investors were using their information in the valuation of a corporation's stock.

Several studies have used the 10-K reports to analyze the tone of words used in the reports (Li, 2010, Feldman, Govindaraj, Livnat & Segal, 2009). The studies concluded that the readability and tone of the reports foreshadow the future profits of a corporation. A 2015 study by Loughran & McDonald cast some doubt on such studies. They claimed that the classification of words as positive or negative was done incorrectly.

While many studies mentioned above focused on data mining techniques to identify words or groups of words associated with risks from the 10-K, some used full sentences (Linsley, Shrives & Crumpton, 2006). Using a full sentence was thought preferable, but coding the data was more time consuming. Although the statements of risk made in mandatory reporting may be difficult to read, they are not done so to conceal risk (Lindsey & Lawrence, 2005). It was also found that reporting risks may actually benefit a corporation.

Studies have discussed the benefit of proper risk disclosure (Hope, Hu & Lu, 2014). Disclosure can help shield the corporation from potential litigation (Dixon & Odoner, 2012). In fact, corporations with high litigation potential report more risks when reporting is voluntary. When risk reporting is required, the disparity in the level of risk reporting decreases (Nelson & Prichard, 2014).

Studying corporations’ reaction to 10-K comment letters sent from the SEC, researchers found that corporations do increase their disclosure when individually contacted about a deficiency (Zahn, 2013). This is consistent with the statements made by the SEC
regarding anecdotal data discussed previously. This is also the premise behind the Realization variable hypothesized in this thesis.

As presented in this literature review, studies have been successfully carried out using quantitative and qualitative data from the 10-K report. While there are similarities between this study and other research projects, this study remains unique as it examines information security risk. Also, it will add to the body of knowledge because no other study of this type has been carried out after the SEC request for cybersecurity risk data and it’s subsequently published guideline. The study is also unique insofar as the study’s sample population will consist exclusively of large U.S. banks, and risks were compared to recognized threats.
RESEARCH METHODS

3.1 Overview

The primary data collection methodology used for this thesis was qualitative data analysis, insofar as it derived data from textual reports. The textual data was then transformed into quantitative data by coding the data into generalized classifications. This quantitative data will then be used for all data analysis.

The study used the final, year-end 10-K report of a sample of the 30 largest commercial banks in the United States for the years 2007 to 2014. The 10-K data was transformed into quantitative data for analysis. While qualitative data projects (such as case studies) are difficult to analyze (Yin, 2003) the use of controls helped assure data validity. One of the controls utilized was a qualitative codebook. The codebook helped ensure that the qualitative data was coded in a consistent manner (Creswell & Clark, 2007).

Once the data from the corporations was coded, the information was categorized. After categorization, each bank's risk data was compared to the threat information collected inductively from the 10-K reports. When there was a match, this was recorded. When all the banks were processed, the number that indicated a match was summed by year and then by entity. The summation was then be divided by the corresponding summation of threats for each particular year.

For instance, if ABC Bank had six risks that matched a corresponding threat, there would be a 6 in the match indicator column. If the threat data indicated 15 threat categories, ABC Bank would then have a matching total of .4 ($\sum \text{risk} / \text{threat}$). Therefore, an entity that
has identified all of the risk for each threat category had a matching percentage (MP) of 1. Conversely, no matches resulted in a MP of 0.

Transforming qualitative 10-K report data into quantitative data is not unique to this study. This is the same technique used in a study to examine the accuracy of self-disclosed material risks (Campbell, Chen, Dhaliwal, Lu & Steele, 2011) and in a study that sought to use the described risk factors as a predictor of cybersecurity incidents (Wang, Kannan & Ulmer, 2013).

The study also used year-end earnings per share data to determine how a profit or loss could affect the accuracy of cyber security risk reporting. This data was collected from standard industry reports for each of the sample corporations. The profits were recorded as a 1 and the losses as a 0.

It was also necessary to capture whether each corporation had experienced an event that resulted in an exploit of a cybersecurity risk. Any significant issues or changes within a corporation that occur between 10-K reporting periods need to be filed on an 8-K report. This report was used to collect cybersecurity incident information. The 8-K reports for the sample were obtained from the SEC’s EDGAR system. The reports were then manually evaluated to determine if the corporation experienced an exploitation of a cybersecurity risk. The factors were recorded as a summation of events for that corporation for the desired year.

Multiple coders were used to help ensure validity. Several 10-K reports were picked at random and given to a second coder. After the reports were coded by both coders, any differences were noted and the necessary changes to the code book were made.
3.2 Project Model

The objective of this research project is to scientifically determine if self-disclosed risk reporting on the SEC mandated 10-K report is accurate. The study also attempts to ascertain factors that may affect the accuracy of the report. This study presents a model illustrating the action of the independent variables on the dependent variable, reporting accuracy.

The goal of the project model was to ascertain if, and to what degree, the described factors affect the reporting accuracy of cybersecurity risk. The proposed model for the interaction is presented in Figure 3.

![Figure 4: Research Model](image)

Each association to the reporting accuracy construct represents a hypothesized relation between the two constructs. The solid lines between the constructs indicate a relationship that is not bound by the timing of an event. The dotted lines indicate that the variable is isolated by
the temporal nature of an event, for instance; the publishing of the guidance document in 2011. The hypotheses are presented below;

- **H1**: Guidance contributes to reporting accuracy
- **H2**: Maturity does occur and contributes to reporting accuracy
- **H3**: Profitable corporations have higher reporting accuracy
- **H4**: A cybersecurity incident will increase reporting accuracy

### 3.3 Theoretical Foundation

This thesis has identified four cause-and-effect relationships that may have a bearing on the accuracy of self-disclosed cybersecurity risks. No single theoretical foundation encompasses each relationship. Therefore, the theoretical foundation for each of the relationships is identified separately.

**Lack of guidance**

**Cause:** Guidance

**Effect:** Increased accuracy in cybersecurity reporting

**Theory:** general deterrence theory

The theoretical basis for this relationship is the General Deterrence Theory (GDT) which states that the perceived likelihood of being caught and the perceived severity of punishment are key decision factors in considering committing an infraction (Gibbs, 1975). In this model, the infraction is intentionally underreporting cybersecurity risk. The punishment would be some legal action initiated by the SEC or stockholders.

Although the SEC asked corporations to include material risks in 2005, corporations were left to determine which risks were material risks. As stated previously, when the
A cybersecurity risk reporting guideline was published in 2011, which, in effect, informed corporations that cybersecurity risks are material risks. Therefore, incorrectly reporting cybersecurity risk violates an SEC directive. This study treats the SEC request for accurate risk reporting as a law and not doing so as an infraction of that law. Treatment of the SEC guideline as a law makes the General Deterrence Theory an appropriate basis for the study.

If the GDT applies to this situation, there should be an increase in reporting accuracy after the 2011 guideline publication. This increase in accuracy would be due to corporations attempting to comply with the SEC’s request. Determining the effect guidance had on reporting accuracy, the number of reported risks was compared from year to year. If guidance was an active phenomenon, there would be an increase in the number of risks being reported after the guidance document of 2011 was published. This construct was analyzed using simple variance analysis and regression analysis using a dummy variable to indicate the year that the guidance document was published.

**Gaining Experience**

**Cause:** Maturity

**Effect:** Increased accuracy in cybersecurity reporting

**Theory:** learning curve

Maturity, in the context of this study, refers to an increase in efficiency and quality of a process over time (Yelle, 1979). The mechanism at work with the Maturity variable is the phenomena of the learning curve. Although the learning curve is predominantly used in manufacturing, it has also been used to analyze the efficiency and quality of management reporting (Yelle, 1979).

If the learning curve phenomenon is present in cybersecurity self-disclosed risk reporting, analysis will show that reporting becomes more accurate as corporations gain
experience. In this study, this phenomenon will be evident if corporate self-disclosure of cybersecurity risk begins to match the actual threat. Because Maturity is a temporal measurement, convergence should increase over time.

Similar to guidance, maturity was analyzed by examining the variance of reported risks from year-to-year. If a maturity effect was occurring, the year-to-year variances would steadily increase. Furthermore, to extricate the maturation effect from other possible variables, regression analysis was performed regressing the number of years of reporting against the number of risks being reported.

**Intentional Underreporting**

**Cause:** Performance

**Effect:** Decreased accuracy in cybersecurity reporting

**Theory:** agency theory

The SEC receives its authority from the 1933 securities and 1934 exchange acts passed by Congress. The acts are general in nature but stress the importance of transparency between the corporations and shareholders. The intent was to provide investors with accurate information regarding their investment in a corporation.

According to the agency theory, the relationship between stockholders and corporate management is one of agent and principal. Stockholders, the principal, delegate the task of running a corporation to the corporate management, the agent. Issues can occur if the goals of the principal and agents are dissimilar (Eisenhardt, 1989). This schism in goals may incent corporate management to underreport unfavorable news in the interests of corporate management.
Therefore, it is in the interests of corporate management to understate corporate cybersecurity risk when they have already reported poor financial performance. In a 2009 study, Kothari et al. (2009) observed that corporate managers delay sharing bad news to investors. While other studies have found no evidence that risk disclosure is related to financial performance (Linsley, Shrives & Crumpton, 2006), the Kothari et al. (2009) used general disclosure statements on which to base their conclusion. This study concentrated on information security risk statements to determine if the agency theory phenomenon is occurring.

In this study, the effect of performance on the accuracy of risk reporting was determined by regressing the profitability of a corporation, calculated using earnings per share data against the number of risks being reported on the 10-K report.

**Awareness of risk**

**Cause:** Realization

**Effect:** Increased accuracy in cybersecurity reporting

**Theory:** agency theory / general deterrent theory

Although corporations should be aware of the cybersecurity risks present within their corporate domain, it is possible they underreport them because they are unaware of them. They may believe that a threat does not apply to them or that they have no exposure. They also may wish to avoid detailing the risk to their stockholders for self-serving purposes as described by agency theory. However, if an undisclosed risk is exploited and exposed to the public, the details of the exploit will need to be revealed.

After an incident, it is possible a corporation will attempt to limit its liability by being vigilant in correctly reporting all risks (Skinner, 1994). General Deterrent Theory would also
apply as a corporation attempts to comply with regulations before they face sanctions. Therefore, if a risk is exposed it is possible that the accuracy of cybersecurity risk reporting will increase.

It was the intent of this study to determine the realization effect on reporting accuracy by performing variance and regression analysis. In this analysis, reporting accuracy would be regressed against a dummy variable indicating if a cybersecurity event occurred. The data indicating that a cybersecurity event occurred would be taken from each of the sample populations’ 8-K report. However, it was found that there were no cybersecurity incidents reported on the 8-K reports for the sample population. This made analyzing the realization effect impossible.

### 3.4 Sample Selection

The intent of the study was to analyze the 10-K reports from the 30 largest publicly traded U.S. banking corporations. Because there are many ways to determine the size of a bank, it was decided that total deposits (publicly available from the Federal Deposit Insurance Corporation (FDIC)) would be used. Deposits were chosen because of the availability of deposit information and its general understandability. To be included in the study, the banking corporations needed to be U.S. corporations subject to mandatory reporting requirements as stated by the SEC. To generate the list of sample banks, the bank name and total deposit information were downloaded from the FDIC. The list was then sorted by total deposit and the top 30 entities selected. The list of sample entities is presented in Table 2.
Table 2: Sample Entities

<table>
<thead>
<tr>
<th>Entity Name</th>
<th>Ticker</th>
</tr>
</thead>
<tbody>
<tr>
<td>JPMorgan Chase Bank, National Association</td>
<td>JPM</td>
</tr>
<tr>
<td>Bank of America, National Association</td>
<td>BAC</td>
</tr>
<tr>
<td>Wells Fargo Bank, National Association</td>
<td>WFC</td>
</tr>
<tr>
<td>Citibank, National Association</td>
<td>C</td>
</tr>
<tr>
<td>U.S. Bank National Association</td>
<td>USB</td>
</tr>
<tr>
<td>PNC Bank, National Association</td>
<td>PNC</td>
</tr>
<tr>
<td>Capital One, National Association</td>
<td>COF</td>
</tr>
<tr>
<td>State Street Bank and Trust Company</td>
<td>STT</td>
</tr>
<tr>
<td>Branch Banking and Trust Company</td>
<td>BBT</td>
</tr>
<tr>
<td>SunTrust Bank</td>
<td>STI</td>
</tr>
<tr>
<td>Fifth Third Bank</td>
<td>FITB</td>
</tr>
<tr>
<td>Regions Bank</td>
<td>RF</td>
</tr>
<tr>
<td>Charles Schwab Bank</td>
<td>SCHW</td>
</tr>
<tr>
<td>Morgan Stanley Bank, National Association</td>
<td>MS</td>
</tr>
<tr>
<td>The Northern Trust Company</td>
<td>NTRS</td>
</tr>
<tr>
<td>Union Bank, National Association</td>
<td>UBSH</td>
</tr>
<tr>
<td>KeyBank National Association</td>
<td>KEY</td>
</tr>
<tr>
<td>Manufacturers and Traders Trust Company</td>
<td>MTB</td>
</tr>
<tr>
<td>Goldman Sachs Bank USA</td>
<td>GS</td>
</tr>
<tr>
<td>Comerica Bank</td>
<td>CMA</td>
</tr>
<tr>
<td>Ally Bank</td>
<td>ALLY</td>
</tr>
<tr>
<td>The Huntington National Bank</td>
<td>HBAN</td>
</tr>
<tr>
<td>E*TRADE Bank</td>
<td>ETFC</td>
</tr>
<tr>
<td>First Niagara Bank, National Association</td>
<td>FNFG</td>
</tr>
<tr>
<td>GE Capital Retail Bank</td>
<td>GE</td>
</tr>
<tr>
<td>City National Bank</td>
<td>CYN</td>
</tr>
<tr>
<td>New York Community Bank</td>
<td>NYCB</td>
</tr>
<tr>
<td>Silicon Valley Bank</td>
<td>SIVB</td>
</tr>
<tr>
<td>Hudson City Savings Bank</td>
<td>HCBK</td>
</tr>
<tr>
<td>Synovus Bank</td>
<td>SNV</td>
</tr>
</tbody>
</table>

3.5 Risk Categories

Because the risks on a corporation’s 10-K report are typically presented in a general manner, it was necessary to combine many risks into condensed categories. The generality of
the categories matched the generality of the risks on the 10-K reports. Here is an example of a corporate risk statement:

“While the Company has policies and procedures designed to prevent or limit the effect of, interruption or of its information systems, there can be no assurances that any such failures, interruptions or security breaches will not occur; or if they do occur, that they will be adequately addressed.”

As presented, the statement does not specifically name any information security risks that could be recognized by an informed reader. However, by analyzing the statement and making inferences about its meaning, it can be inferred that the corporation is stating they are disclosing risks about computer maintenance and system hacking or cracking. This inductive conclusion was reached by examining the terms “failure” and “security breach” in the statement.

This inductive categorization process was completed by reading each statement and then referring to a catalog of previously classified statements. Use of a catalog reduced the possibility of miscoding a statement (Creswell & Clark, 2007). Although time consuming, the process was not be possible using data mining or other methods, that is searching for keywords or strings of key words.

After reviewing each of the 30 organizations 10-K reports for the 2007 – 2014 periods, the risk statements were reduced to the categories presented in Table 3.
Table 3: Risk Categories

<table>
<thead>
<tr>
<th>Risk Categories</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration / Architecture</td>
</tr>
<tr>
<td>Denial of Service</td>
</tr>
<tr>
<td>Hacking / Cracking activity</td>
</tr>
<tr>
<td>Identity Theft</td>
</tr>
<tr>
<td>Insider</td>
</tr>
<tr>
<td>Maintenance</td>
</tr>
<tr>
<td>Malware</td>
</tr>
<tr>
<td>Mobile issues</td>
</tr>
<tr>
<td>Phishing / Email attacks</td>
</tr>
<tr>
<td>Social Engineering</td>
</tr>
<tr>
<td>Third Party</td>
</tr>
<tr>
<td>Virus – Computer</td>
</tr>
</tbody>
</table>

Risk statements regarding environmental, natural disasters, terrorism, pandemic, or war were not included in this study. While they may be risks to the corporation, they are not specific enough to categorize as an actual threat. Furthermore, the inclusion of terrorism, war, etc. on the 10-K report has been seen as a reaction to events and not as an actual risk to a corporation (Robbins & Rothenberg, 2005). If the study were to include natural disaster risk, the risk data would be skewed by organizations whose geographical locations put them at high risk for natural disasters, for example hurricanes or earthquakes.

The derived risks categories - with the exclusion of the afore-mentioned risks do, at face value, match the threats facing an organization doing business in the current online environment. However, it is still beneficial to use multiple sources to provide validity to the derived data (Yin, 2003). To this end, an attempted to find a list of information security
threats that were generalized enough to match the risk categories was conducted. Most threat category data found in the domain literature was either too specific or too general to match the risk categories created out of the study.

It was difficult to find studies that had categorized information security risks. Most studies such as Bao (2013), grouped information security risk into procedural categories such as operational disruption. For this reason, it was not possible to validate the risk categories using convergent validity techniques.

### 3.6 Data Collection

The majority of the 10-K data was obtained from the SEC’s Edgar system. Some organizations, such as Wells Fargo and U. S Bank, do not include information security risks on their 10-K report. They refer to their annual report as the source for this information. Referring to the annual report for risk disclosure is allowed by the SEC. It was therefore necessary to download the annual report from each of these entities’ websites.

To ensure that the correct data was downloaded from the Edgar system, the forms file was obtained. This file contains a list of uploaded documents for each quarter. Figure 5: SEC Forms file, is a sample from this file.

<table>
<thead>
<tr>
<th>10-K</th>
<th>1ST CONSTITUTION BANCORP</th>
<th>1141887</th>
<th>2014-03-31</th>
<th>edgar/data/1141887/0001146693-14-002338.txt</th>
</tr>
</thead>
<tbody>
<tr>
<td>10-K</td>
<td>1ST SOURCE CORP</td>
<td>34782</td>
<td>2014-02-21</td>
<td>edgar/data/34782/00000034782-14-000888.txt</td>
</tr>
<tr>
<td>10-K</td>
<td>1st Century Bancshares, Inc.</td>
<td>1428515</td>
<td>2014-03-07</td>
<td>edgar/data/1428515/0001457745-14-003615.txt</td>
</tr>
<tr>
<td>10-K</td>
<td>1st FRANKLIN FINANCIAL CORP</td>
<td>38723</td>
<td>2014-03-31</td>
<td>edgar/data/38723/0001376474-14-000084.txt</td>
</tr>
<tr>
<td>10-K</td>
<td>1st United Bancorp, Inc.</td>
<td>1415277</td>
<td>2014-02-10</td>
<td>edgar/data/1415277/0001172000-14-000011.txt</td>
</tr>
<tr>
<td>10-K</td>
<td>22nd Century Group, Inc.</td>
<td>1347658</td>
<td>2014-01-30</td>
<td>edgar/data/1347658/0001144204-14-004965.txt</td>
</tr>
<tr>
<td>10-K</td>
<td>24HOLDINGS INC</td>
<td>1025315</td>
<td>2014-03-26</td>
<td>edgar/data/1025315/0001144204-14-017898.txt</td>
</tr>
</tbody>
</table>

**Figure 5: SEC Forms File**
Because the data is reported with a three month delay, the first quarter data contains the year-end data for the entity. The file for years 2007 – 2014 was obtained. This file was then truncated to include only the 10-K forms for the entities of interest. Because the file included the full path for the desired reports, it was possible to write selective FTP download scripts to obtain both the 10-K and 8-K data. An example of the FTP script used for the download process is presented in Figure 6: Selective FTP Script.

Because the download included many files, it was necessary to schedule downloads during weekend evenings. Scheduling downloads during off hours was suggested by the EDGAR administrators as a way to prevent a system slowdown for other users of the EDGAR system.

The downloaded files ranged in size from 1 to more than 130 megabytes in size and occupied nearly 14 GB on the retrieval disk. The larger files contained hundreds of pages of information. While the files were stored and downloaded as text files, they were formatted as
html. Because of the size, it was not possible to review the data in a text editor. The files had to be converted to html so they could be viewed in a web browser.

Viewing the files in a web browser made it possible to take advantage of the hyperlinks within the document. This facilitated navigation to section “Item 1A Risk Factors” easily. Figure 7: Sample 10-K Hyperlinks, is a sample of the presentation of the 10-K reports index feature with hyperlinks. Not all 10-K reports had hyperlinks. For reports without hyperlinks, it was necessary to perform a textual search for the correct section of the report.

Yearly earnings per share data were utilized to determine if the entity had a profit or loss for the reporting year. This information was downloaded for each entity from Morning Star Financial. Morning Star is a company that provides freely available financial information to the public. However, as stated previously, this information is public and could have come from a variety of sources.

After the data was downloaded it was matched to the correct entity and entered into a database created for collection of the study data.
3.7 Data Transformation

A total of 240 10-K reports were used for the study. That number represents 30 entities for a period of 8 years. Each report had the possibility of populating 12 risk categories and therefore 2,880 possible entries.

Each 10-K report was examined to determine which information security risks the organization was disclosing. According to the guideline published by the SEC, information security risk should be identified in section “1A Risks” of the 10-K report (SEC, 2014). Thus, this section was the focus of the examination. The report was read much the same way an investor would read any financial report. The risk section was reviewed for headings that could contain risk reporting information. Attention was then focused on those sections for analysis.

Information security risk statements were often intermixed with general operational risk statements. Operational risk statements mentioning fraud, unauthorized transactions, or process breakdown were not included in this study. It was important to separate the general operational statements from those about information security. This was done by thoroughly reading the statements to ensure that the reports were discussing their computer systems. Risks related to manual processes or operational controls, such as checks and balances, were not included in this study.

As each section was analyzed, information security risk data was collected into a database using a data entry application developed for the task. Figure 8: Data Entry Application is a screen capture of the data entry application’s input form.
Along with facilitating data input, the data entry application also provided data integrity functions. Those functions included choosing risk categories from a dropdown box to prevent the possibility of mistyping a category name. Furthermore, the data input into the main data collection table was created using a composite primary index key. The primary index key is comprised of the reported year and the risk category. Because this is a primary key, there is no possibility of duplicate entries within the main collection table.

Another integrity task the data input application facilitates is a display of the entity name. During data collection, it was possible to match the entity name on the database to the 10-K report being coded. The application also includes the reporting date, file name, and path where the data for the particular organization is located.
After the data was collected, the risk incident categories for each of entities by year were summed as illustrated in Table 4: Summation of Risk Categories presented below. (See Appendix A for full list).

**Table 4: Summation Risk Categories**

<table>
<thead>
<tr>
<th></th>
<th>2007</th>
<th>2008</th>
<th>2009</th>
<th>2010</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bank of America</td>
<td>5</td>
<td>5</td>
<td>6</td>
<td>7</td>
</tr>
<tr>
<td>Citibank</td>
<td>4</td>
<td>2</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Wells Fargo</td>
<td>7</td>
<td>6</td>
<td>5</td>
<td>6</td>
</tr>
</tbody>
</table>

The final summation is the quantitative data used in the data analysis section of this thesis. Because statements of self-disclosed risks were categorized, it was also possible to analyze categorized data. Table 5:, is a sample of a report that utilizes categorized data (see Appendix A for full listing).

**Table 5: Summation of Risk**

<table>
<thead>
<tr>
<th></th>
<th>2007</th>
<th>2008</th>
<th>%Var</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration</td>
<td>12</td>
<td>14</td>
<td>17%</td>
</tr>
<tr>
<td>DOS</td>
<td>1</td>
<td>1</td>
<td>0%</td>
</tr>
<tr>
<td>Hack</td>
<td>7</td>
<td>10</td>
<td>43%</td>
</tr>
</tbody>
</table>

### 3.8 Validity

As with any scientific study, validity must be considered. Furthermore, studies that incorporate qualitative data often have issues not seen in a strictly quantitative study (Yin, 2003). It was therefore important to establish guidelines that ensure proper controls. This study employed a variety of methods to guarantee rigor regarding validity.
The first validity methodology used was complete documentation of the coding and categorization criteria of the qualitative data. This was accomplished by creating and maintaining a coding catalog. The catalog criteria are stored in a database and all ambiguous coding decisions were made by referring to this catalog. This disciplined coding approach provided for transparency and replication of the coding process.

Replication allowed multiple coders to validate the coding process. Operationally, this was accomplished by providing a random selection of qualitative data to a second coder. The second coder utilized the coding catalog to code the random sample. Differences between the two coder’s data were noted and discussed between coders occurred before a final coding occurred. The catalog was then adjusted to remove the ambiguity that caused the discrepancy.

Another validity process that was employed was the review of a random sample of 10-K reports. To this end, a random sample of 10-K were reexamined to determine if the sample was coded correctly. 4% of the reports were reanalyzed representing 120 entry points. The analysis resulted in an error rate of less than 1%. Any discrepancies were reviewed and adjustments were made to the sample data.

The random reports chosen for reanalysis were selected by numbering each report and using a random number function to select the number that corresponded to the report. This methodology ensured that the samples were chosen at random.

Additional validity efforts, such as determining convergent and discriminate validity, were accomplished by comparing the constructs and their proceduralization with other studies. Although this is a unique study, other projects have used similar constructs for their research endeavors. Two such studies are those conducted by Wang, Kannan & Ulmer, 2009 and Campbell, Chen, Dhaliwal, Lu, Steele, 2011. Both studies used risks data from the 10-K
report. The studies then categorized the data using techniques specific to their study. The Wang study focused on the context of the statement and the Campbell study focused on the type of risk.

Both studies were able to illustrate predictive validity. Using the 10-K data, the Wang study was able to predict the occurrences of a breach announcement by a study entity. The Campbell study was able to associate risk disclosure with an actual occurrence associated with the disclosed risk.

### 3.8.1 Coding Catalog

As mentioned previously, a coding catalog was created to provide consistency for ambiguous statements. While some of the risk statements were straightforward, that is those, indicating disclosure of the risk of a virus, malware, or denial of service attack; other statements were less definitive, thus making coding more difficult. The coding catalog created specified a keyword or phrase with a corresponding category. An excerpt from the coding catalog is presented in Table 6: (see Appendix C).

<table>
<thead>
<tr>
<th>10-K expression</th>
<th>Threat Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account takeovers</td>
<td>Identity theft</td>
</tr>
<tr>
<td>Breach</td>
<td>Hack</td>
</tr>
<tr>
<td>Cyber Attacks</td>
<td>Hack</td>
</tr>
<tr>
<td>Degradation of service</td>
<td>DOS</td>
</tr>
<tr>
<td>e-Fraud</td>
<td>Identity theft</td>
</tr>
<tr>
<td>Electrical Outage</td>
<td>Not included. This is a business continuation issue</td>
</tr>
<tr>
<td>Employee Tampering</td>
<td>Insider</td>
</tr>
<tr>
<td>Employee tampering</td>
<td>Insider</td>
</tr>
</tbody>
</table>
To understand the construction of a coding catalog it is necessary to define a code. Put simply, in qualitative data analysis a code is a word or phrase that summarizes an idea or salient point involved in the analysis (Saldana, 2008). Because the interest of this study is cybersecurity sometimes otherwise referred to as information security, the salient statements were all related to an entity’s computer system. This allowed statements not related to the computer system to be ignored.

While some coding can be completed for the purposes of discovery (Saldana, 2008) this study did not utilize a heuristic coding methodology. Also, categories are often determined after an initial coding of the data has been completed (Saldana, 2008). However, because this study has a specific scope, statements were immediately coded into categories.

Although the coding categories were determined inductively, they were primarily determined by explicit declaration of a specific risk. This therefore reduced the amount of interpretation required to determine coding categories.

Some of the unambiguous statements examined were easy to categorize. For instance, the statement “attacks could degrade the availability of our online banking system” was coded as Denial of Service. Other statements such as “Spam attack” were more difficult to categorize. The statement “Spam attack” could be viewed as a denial of service attack or an e-mail attack such as phishing. The decision in this case was to categorize this statement as the risk of an e-mail based attack. This was determined to be the most likely intent of the report writer. This model of most likely intent was used for categorizing all of the ambiguous statements encountered.
RESULTS AND DISCUSSION

4.1 Dataset

The goal of the data analysis was to determine if, and to what degree, the described factors affect the reporting accuracy of cybersecurity risks. It is hypothesized that each of the factors acts independently on reporting accuracy. Therefore, the study consisted of four independent variables representing these factors: guidance, maturity, performance, and realization. The dependent variable was the accuracy of cybersecurity risk reporting.

The independent variables were longitudinal, with values collected for each year from 2007 to 2014. Because there was a reasonable amount of data and no missing data, panel data analysis was an appropriate technique for this-time series study (Torres-Reyna, 2010). Analyzing panel data enables treating each time period as a separate variable. This allowed for the analysis of guidance and maturity constructs as a function of the variance between time frames. It was also possible to use a dummy variable that represents the number of years of maturity and guidance.

The dependent variable, reporting accuracy, was the percentage of risks matched to threats for each period. It was then possible using regression analysis to determine the correlation coefficient of the independent variables performance and realization as they are regressed against the dependent variable reporting accuracy.

Examining the variances between periods provided data about how maturity affects reporting accuracy. This is the same technique that was used to determine the effect of the guidance factor. The guidance factor does not manifest until 2011. Therefore, the variance of reporting accuracy between 2011 and 2014 is the effect of guidance on the matching
percentage. The coefficients determined for each factor were added to the model. Analysis of the completed model fulfills the goals of this project.

When dealing with longitudinal data, it was difficult to understand its full meaning without being aware of the events that occurred during the data collection timeframe. The following timeline is presented as a convenient point of reference.

As indicated by the timeline, there were many events occurring throughout the period of study. Some of the events were likely to affect the rate at which entities report information security risks. By using a longitudinal data analysis technique such as panel data analysis, it is possible to utilize some of the events as variables in our analysis, for instance, guidance. In late 2011, the SEC published a guidance document instructing entities how to report information security risks. Therefore, an effect of the guidance in the 2011 - 2014 data would be observed.
To incorporate the effect of guidance in a regression model, it was necessary to create a dummy variable named “guide.” This variable was valued at zero for all years from 2007 through 2010. The years after the guidance was published have the “guide” variable valued at 1. The “guide” variable allowed the process to identify those values that occurred before and after the published SEC guidance document of 2011.

This same dummy variable methodology was also used for the Maturity variable. Maturity, being a variable theorized by the phenomena of the learning curve, occurs continuously. The occurrence of Maturity is evident by report writers gaining experience in report creation from year to year. By using a dummy variable name “mat_1,” it was possible to indicate the maturity of each data point to the regression model. For instance, in year 2007, the “mat_1” value was 1 in 2007 the value was 2. The “mat_1” variable was incremented through each year of the study. The column named “cik” was the unique identifier for each of the subject entities. The threat column was the summation of the threat for that entity by year. The “match” was the percentage of risks matched to threats for that entity in that year. The “eps” column indicates the actual earnings per share number where the “eps_ind” was a 1 for a profit and 0 for a loss.

An illustration of the resulting data set used for analysis is presented in Table 7.
Table 7: Dataset Sample

<table>
<thead>
<tr>
<th>year</th>
<th>cik</th>
<th>threat</th>
<th>match</th>
<th>eps_ind</th>
<th>eps</th>
<th>mat_1</th>
<th>guide</th>
</tr>
</thead>
<tbody>
<tr>
<td>2007</td>
<td>18349</td>
<td>5</td>
<td>41.67</td>
<td>1</td>
<td>11.2</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>2007</td>
<td>19617</td>
<td>4</td>
<td>33.33</td>
<td>1</td>
<td>4.38</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>2007</td>
<td>28412</td>
<td>0</td>
<td>0.00</td>
<td>1</td>
<td>4.43</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>2007</td>
<td>35527</td>
<td>4</td>
<td>33.33</td>
<td>1</td>
<td>1.99</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>2007</td>
<td>36104</td>
<td>3</td>
<td>25.00</td>
<td>1</td>
<td>2.43</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>2007</td>
<td>36270</td>
<td>0</td>
<td>0.00</td>
<td>1</td>
<td>5.95</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>2007</td>
<td>40545</td>
<td>0</td>
<td>0.00</td>
<td>1</td>
<td>2.17</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>2007</td>
<td>40729</td>
<td>2</td>
<td>16.67</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>2007</td>
<td>49196</td>
<td>1</td>
<td>8.33</td>
<td>0</td>
<td>0.25</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

This dataset is considered to be in a long format, indicating there is an individual row for each interval. The corresponding wide format would see the time interval as a column of data. Furthermore, the dataset is considered highly balanced, indicating there are no missing values.

4.2 Data Analysis

While some of the simple data analysis was conducted using Microsoft Excel, the tool chosen to perform the advanced statistical analysis was a commercially available package named Stata created by Stata Corporation. Stata was chosen primarily for its ability to easily analyze panel data. Stata also has a large user community and a support staff to help with technical or analytical issues.

While several regression analysis techniques were considered, panel data analysis with fixed effect appeared to be the most appropriate methodology. This method was chosen because there is longitudinal data for each entity and the focus is on variables across time. Panel data analysis works effectively for this type of analysis because it controls for time invariant variables (Baltagi, 2008).
To further justify the decision to use fixed effects analysis, the data was subject to the Hausman test, which determines if the unique error is correlated with the regressor (Greene, 2009). If the error is correlated, the random / single-level mixed method of analysis may be more appropriate form of analysis than the fixed method. The results of the Hausman test are included in Table 8:

Table 8: Hausman Test Output

<table>
<thead>
<tr>
<th></th>
<th>Coefficients</th>
<th>(b)</th>
<th>(B)</th>
<th>(b-B)</th>
<th>sqrt(diag(V_b-V_B))</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>(b)</td>
<td>(B)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>f01</td>
<td>f01</td>
<td>r01</td>
<td>r01</td>
<td></td>
<td></td>
</tr>
<tr>
<td>eps_ind</td>
<td>0.6621188</td>
<td>0.4680688</td>
<td>0.19465</td>
<td>0.4696708</td>
<td></td>
</tr>
<tr>
<td>mat_1</td>
<td>5.505518</td>
<td>5.503901</td>
<td>0.001671</td>
<td>0.0377901</td>
<td></td>
</tr>
<tr>
<td>guide</td>
<td>9.112059</td>
<td>9.152486</td>
<td>-0.0404271</td>
<td>0.1980973</td>
<td></td>
</tr>
</tbody>
</table>

b = consistent under Ho and Ha; obtained from xtreg
B = inconsistent under Ha, efficient under Ho; obtained from xtreg

Test: Ho: difference in coefficients not systematic

\[
\text{chi2}(3) = (b-B)'[(V_b-V_B)^{-1}](b-B) = 0.17
\]

\[
\text{Prob} > \text{chi2} = 0.9822
\]

The results of the Hausman test indicated that there was little difference in the coefficients from the fixed and random analysis methods. Furthermore, we have a high degree of significance as the value of chi-squared is 0.9942, indicating that the fixed effects model is appropriate.

The dataset was also been tested for autocorrelation using the Woodridge test. The output of that test is below in Table 9: Since the outcome of the test is insignificant, we assume that we are not seeing an autocorrelation effect.
Table 9: Woodridge Autocorrelation

```
.xtserial match mat_1 eps_ind guide

Wooldridge test for autocorrelation in panel data
H0: no first-order autocorrelation
F(  1,    29) =   9.048
Prob > F =  0.0054
```

The data was also tested for heterogeneity as shown in Figure 10, indicating that there were considerable differences in the mean of the dependent variable, thus resulting in an upward progression. This result is further supported by the data analysis.

![Figure 10: Heterogeneity Variable by Year](image)

Finally, the data was tested for heteroskedasticity. While the test is included on Table 10, the nature of the independent variables means it has very little meaning. The reason for this lack of meaning is the independent variables, which are considered dummy variables and
simply mark either the timing of an event or the profit or loss during a period. For this same reason, scatter graphs are of little use as they show only the value of the dummy variable. In the interest of completeness, the scatter diagrams are included in Appendix D.

Table 10: Data Heteroskedasticity

```
. xttest3

Modified Wald test for groupwise heteroskedasticity
in fixed effect regression model

H0: sigma(i)^2 = sigma^2 for all i

chi2 (30) = 888.81
Prob>chi2 = 0.0000
```

4.2.1 Reporting Accuracy Analysis

Corporations determine cybersecurity risks by evaluating likely attacks against resource vulnerabilities that could result in an unfavorable event (Stoneburner, Goguen & Feringa, 2002). Generally, all threats within a specific domain should elicit the recognition of a risk as illustrated in Figure 11.

![Figure 11: Matched Threat Illustration](image)
If a risk is not disclosed on the 10-K report, it may indicate that an entity is unaware of the threat, or does not want to disclose the threat. An unmatched threat is illustrated in Figure 12.

In this study, the threats within our domain of study have been assigned a category name. Therefore, an unmatched threat represents a risk that an entity has not disclosed to its stockholders. Examining the percentage of self-disclosed risks to threats gives us an idea of how accurate an entity self-disclosed risk reporting is on its 10-K reports. For this reason, the study examined the matching percentage of each entity.

After coding and categorization of the 10-K reports was completed, a matching percentage was calculated for each entity. The matching percentage was calculated as follows:

\[
\frac{\sum \text{Reported Risks}}{\sum \text{All Categories}}
\]

The percentages for each entity were then averaged and sorted by year. The results are presented below in Table 11.
As presented in the table, in 2007 the average matching percentage of the 30 entities was 20.56%. Therefore, of the 12 risk categories included in this study, only 2 or 3 were reported. This percentage increased progressively through the years until we come to 2014, where an average 66.67% of risks were self-disclosed. Furthermore, the standard deviation has decreased from 16.77 to 15.81 indicating there is less variance in each entity’s matching percentage.

Analysis of the matching percentage indicates that entities were reporting more information security risks than previous years. Also, more companies were reporting an increased amount of risk. While this is indeed encouraging, the numbers also indicate that companies were still underreporting information security risks by 33% or approximately four risk categories.

Although the number of reported risks was increasing, there is still enough evidence to assert that, as of 2014, the self-disclosed information risk reporting of large U.S. banks is inaccurate. This inaccuracy began as early as 2007 and continued to a lessening degree through all 8 years of the study. The analysis of the data further demonstrated that none of the study subject entity’s reported 100% of the risk categories on their 10-K reports. The entities highest percentages of reported risks in 2014 were 92% and 83%. The complete list of entities and accuracy percentages are in Appendix A.

Table 11: Cumulative Matching Percentage

<table>
<thead>
<tr>
<th></th>
<th>2007</th>
<th>2008</th>
<th>2009</th>
<th>2010</th>
<th>2011</th>
<th>2012</th>
<th>2013</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average</td>
<td>20.56</td>
<td>23.61</td>
<td>29.17</td>
<td>32.78</td>
<td>46.11</td>
<td>56.11</td>
<td>62.22</td>
<td>66.67</td>
</tr>
<tr>
<td>Median</td>
<td>20.83</td>
<td>25.00</td>
<td>33.33</td>
<td>37.50</td>
<td>50.00</td>
<td>58.33</td>
<td>62.50</td>
<td>66.67</td>
</tr>
<tr>
<td>StdDev</td>
<td>16.77</td>
<td>17.09</td>
<td>18.10</td>
<td>17.73</td>
<td>17.18</td>
<td>19.59</td>
<td>16.49</td>
<td>15.81</td>
</tr>
</tbody>
</table>
4.2.2 Maturity Analysis

The 10-K report data being analyzed for this study spans eight years, from 2007 through 2014. During this period it is likely that those creating the 10-K reports became more proficient in their creation. This proficiency would be noticeable in more accurately reporting the information security risks that an entity faces. This phenomenon of increased efficiency and accuracy is based on the learning curve theory.

The simplest analytical methodology to detect the learning curve phenomenon within the study sample is to calculate the variance of cumulative matching percentage from year to year. The calculation for this variance is as follows:

\[
\frac{\sum \text{Risks}_{\text{Year } 2} - \sum \text{Risks}_{\text{Year } 1}}{\sum \text{Risks}_{\text{Year } 1}}
\]

Table 12: Cumulative Matching Variance, represents the variance for each year of the study data.

<table>
<thead>
<tr>
<th></th>
<th>2007</th>
<th>2008</th>
<th>% Var</th>
<th>2009</th>
<th>2010</th>
<th>% Var</th>
<th>2011</th>
<th>% Var</th>
<th>2012</th>
<th>% Var</th>
<th>2013</th>
<th>% Var</th>
<th>2014</th>
<th>% Var</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Matching</td>
<td>74</td>
<td>85</td>
<td>15%</td>
<td>105</td>
<td>24%</td>
<td>118</td>
<td>12%</td>
<td>166</td>
<td>41%</td>
<td>202</td>
<td>22%</td>
<td>224</td>
<td>11%</td>
<td>240</td>
</tr>
</tbody>
</table>

As demonstrated by the data, each year there is a positive increase in variance thus representing an increase in the number of cumulative risks being reported. Between 2007 and 2008 we see an increase in reported risks of 15%. The final year of data, 2014 realizes an
increase of 7% over the previous year. Figure 13, helps to illustrate the progression of increasing disclosure.

![Figure 13: Total Matching by Year](image)

While it may be tempting to attribute all of this variance to the learning curve, that would be inaccurate. Other factors play a role in the increasing number of risks being reported. Therefore, in an attempt to extricate the learning curve (maturity) effect from other factors, we enlist regression analysis techniques.

Performing a regression analysis on the panel data using the matching percentage as the dependent variable and guidance, maturity, and performance as independent variables resulted in the output presented in Figure 14.
Figure 14: Regression Analysis

The fixed effects panel data regression calculation for the regression analysis is presented below:

\[ Y_{it} = \beta_1 X_{1it} + \beta_1 X_{2it} + \beta_1 X_{3it} + \alpha_i + u_{it} \]

When

\( Y \) = Matching Percentage
\( X1 \) = Performance
\( X2 \) = Guidance
\( X3 \) = Maturity
\( I \) = Entity
\( t \) = Time
\( \beta1 \) = Coefficient for independent variable
\[ \alpha_i = \text{Unknown intercept for each subject entity} \]

\[ u_{it} = \text{Error} \]

As illustrated by the output, all of observations were included for the model and grouped by entity. Also, it was determined that the model is valid by checking that all of the coefficients are different from zero as “Prob > F” is less than .05. Other pertinent information regarding maturity is summarized in Table 13.

**Table 13: Maturity Regression Values**

<table>
<thead>
<tr>
<th>Indicator</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Coef</td>
<td>Coefficients of the regressor indicate the increase in “matching” when maturity is increased by one year.</td>
<td>5.50</td>
</tr>
<tr>
<td>t</td>
<td>t-Value tests to determine if coefficients are different from zero. For 95% accuracy this value should be &gt; 2.045</td>
<td>8.59</td>
</tr>
<tr>
<td>P&gt;</td>
<td>t</td>
<td></td>
</tr>
</tbody>
</table>

As the table above indicates, Maturity was a major determinant of the number of risks reported by an entity. In fact, for every year of maturity, the number of risks reported increases by more than 5 percentage points. Additionally, by examining the “t” and “P>|t|”
indicators we can determine that maturity has a significant influence on the number of risks being reported by our test entities.

### 4.2.3 Performance Analysis

Another variable that was hypothesized to affect the number of risks reported by each entity is the profitability of an entity. It was hypothesized that when a company is profitable it is more inclined to disclose bad news such as an increase in information security risk. This variable was added to the regression analysis mode and the pertinent results are in Table 14.

<table>
<thead>
<tr>
<th>Indicator</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Coef</td>
<td>Coefficients of the regressor indicate the increase in “matching” when performance is one.</td>
<td>0.66</td>
</tr>
<tr>
<td>t</td>
<td>t-Value tests to determine if coefficients are different from zero. For 95% accuracy this value should be &gt; 2.045</td>
<td>0.27</td>
</tr>
<tr>
<td>P&gt;</td>
<td>t</td>
<td></td>
</tr>
</tbody>
</table>

The performance variable tells an entirely different story from the maturity variable. In fact, the results from the “t” and “P>|t|” indicate that the performance variable has no effect
on the dependent variable, therefore indicating that an entity’s performance does not affect the number of risks being reported. To determine if the insignificance of performance is due to intercorrelation, a correlation table of the independent variables was run. See Table 15: Correlation Table.

Table 15: Correlation Table

<table>
<thead>
<tr>
<th></th>
<th>eps_ind</th>
<th>mat_1</th>
<th>guide</th>
</tr>
</thead>
<tbody>
<tr>
<td>eps_ind</td>
<td>1.0000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>mat_1</td>
<td>0.1947</td>
<td>1.0000</td>
<td></td>
</tr>
<tr>
<td>guide</td>
<td>0.2372</td>
<td>0.8729</td>
<td>1.0000</td>
</tr>
</tbody>
</table>

As indicated above, the marker that identifies performance, “eps_ind” is not highly negatively correlated with either of the other independent variables. This fact, combined with the low significance of the variable, indicates that performance is not significant in determining the number of reported risk. Therefore for the performance variable we must accept the null hypothesis that performance does not affect risk reporting.

This result is not unprecedented. A 2006 study examined Canadian and UK banks in regard to risk disclosure and profitability. Although the study examined all reported risks and the banks were from the UK and Canada, they too concluded that there was no correlation between profitability and risk disclosure (Linsley, Shrives & Crumpton, 2006).

4.2.4 Guidance Analysis

As mentioned previously in this thesis, yielding to Congressional pressure the SEC published a guideline for reporting information security risk. This guideline was released to
the public in October of 2011. Because the sample entities did not file their mandatory reporting for the 2011 until the first quarter of 2012, the effect of the SEC guidance would be apparent in 2011 reporting. Therefore, this effect will be seen from 2011 until the last year of this study, 2014.

Referring to Figure 15, there is a sharp increase in reported information security risk in the 2011 10-K reports. The increase is 41% over what was reported in 2010. This increase is the largest single year increase that we see throughout this study. The positive variance is nearly 100% higher than the next highest increase occurring in 2009.

![Figure 15: Total Matching with Guidance](image)

At face value, it certainly appears that Guidance has a significant effect on the amount of information security risk reported. However, the increase in 2011 also includes the other independent variables under study. Therefore, we can refer to the regression analysis numbers to confirm the significance of the Guidance variable. The regression information for guidance is presented in Table 16.
### Table 16: Guidance Regression Values

<table>
<thead>
<tr>
<th>Indicator</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Coef</td>
<td>Coefficients of the regressor indicate the increase in “matching” after the Guidance document was published</td>
<td>9.11</td>
</tr>
<tr>
<td>t</td>
<td>t-Value tests to determine if coefficients are different from zero. For 95% accuracy this value should be &gt; 2.045</td>
<td>3.06</td>
</tr>
<tr>
<td>P&gt;</td>
<td>t</td>
<td></td>
</tr>
</tbody>
</table>
information security risk incidents reported. However, according to Pelroth (2012), there were several subject entities that did have information security incidents as reported by the media.

Six banks had experienced sustained denial of service attacks during the week of September 24, 2012. These banks were part of this study sample population: Bank of America, JP Morgan Chase, Citigroup, U.S Bank, Wells Fargo, and PNC Bank. Comparing the reported denial-of-service risk reported between 2011 and 2012 we see the following results in Table 17: Selected Entity 2011, 2012 DOS.

<table>
<thead>
<tr>
<th>Name</th>
<th>Ticker</th>
<th>DOS 2011</th>
<th>DOS 2012</th>
</tr>
</thead>
<tbody>
<tr>
<td>JPMorgan Chase Bank, National Association</td>
<td>JPM</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Bank of America, National Association</td>
<td>BAC</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Citibank, National Association</td>
<td>C</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>PNC Bank, National Association</td>
<td>PNC</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Wells Fargo Bank, National Association</td>
<td>WFC</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>U.S. Bank National Association</td>
<td>USB</td>
<td></td>
<td>x</td>
</tr>
</tbody>
</table>

As Table 17, indicates, prior to the publicized DOS attacks, only two of the entities reported a risk of DOS. However, after the attacks occurred, all six of the entities reported DOS as a risk on their 10-K reports.

Further indication that the Realization phenomena may be occurring comes in the wake of the Target data breach of 2013. In 2013, Target announced a data breach that exposed millions of customers’ financial data. The vector of the breach was malware on Target’s point of sale systems (Constantin, 2014). If Realization is occurring, we would expect an increase in the reporting of malware risk in 2013. Table 18: Malware Reported after Target Breach, indicates the number of entities that reported malware risk from 2011 – 2014.
The results indicate there was a 45% increase in the reporting of malware after this announcement. This was followed by only a 12% increase the following year.

While the result of this analysis gives some credence to the effect of Realization, it is only anecdotal evidence. Because security incident information was not available on the 8-K reports, it would be necessary to thoroughly search all media to do a successful scientific study. Because this was beyond the scope of this study, validation of the realization variable was abandoned.

### 4.3 Completed Model

The model presented in Figure: 16 indicate the correlation strength of the independent variables to the dependent variable.

<table>
<thead>
<tr>
<th>Malware</th>
<th>2011</th>
<th>2012</th>
<th>2013</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malware</td>
<td>8</td>
<td>11</td>
<td>16</td>
<td>18</td>
</tr>
</tbody>
</table>
The insignificant independent variables are removed and the final model is presented in Figure 17. This indicates that both maturity and guidance have a significant effect on reporting accuracy of the 10-K report. Thus the null hypothesis is rejected for both Hypothesis 1 and 2.
CONCLUSIONS

While the term accuracy is subjective, this study found that in 2014 the study entities did not report 33% of the risks found within their domain of business. The number of reported risks steadily climbed throughout the study period. This increase in risk reporting is an encouraging sign. However, it is up to the bank regulating authorities to determine if including 66% of risks makes the report accurate.

Two factors were found to have an effect on the reporting accuracy of information security risk. The first factor was maturity. As entities gained experience in reporting risks, the accuracy of their reporting increased. The other factor was guidance. When the SEC published a guidance document telling companies what to report and how to report it, accuracy increased.

The effect of maturity on reporting accuracy was not unexpected. As presented earlier in this thesis, the feasibility of applying learning curve theory to management reporting has been established. However, increasing the accuracy of risk reporting not only required organizations to learn how to report but also required them to learn more about their corporation. By learning more about the risk they face, corporations will be in a better position to mitigate those risks.

The increase in reporting accuracy due to guidance is an important finding. It shows how a simple instruction can increase the accuracy of risk reporting. While this study focused on information security risk, guidance could be used for other risks as well. Also, the SEC published the guideline without implementing additional legislation. If it were necessary for the SEC to seek new legislation, the objective would have been substantially delayed or even dismissed by a vote of congress.
The study also demonstrated that entities’ profitability had no effect on the accuracy of information security risk reporting. This result was previously observed in studies with different types of risk. It is therefore not surprising that accuracy information security risk reporting is not dependent on entities’ profitability.

Although the study presented anecdotal data to show that reporting of a specific risk increased with the realization of that risk, it could not be studied scientifically. The scope of the study would have had to change considerably to facilitate a scientific study of this hypothesized phenomenon.

5.1 Future Work

In many ways this study can be viewed as a proof of concept. The study reviewed self-disclosed information security risk from the SEC-mandated 10-K report and got meaningful results. However, the study was limited to large U.S. banks. Additional studies could use a random sample of all publicly traded corporations regulated by the SEC to provide a generalizable result.

Publicly traded corporations should be reporting incidents such as security breaches on their 8-K reports, but they are not doing so. This lack of reporting prevented scientifically determining whether realization of a threat increased the likelihood of reporting that threat’s corresponding risk. Another study could be undertaken that would circumvent this lack of 8-K reporting by using other means, such as news reports, to determine which threats were becoming known as a result of a publicized breach.
Because of the general nature of the risk statements made on the 10-K report, risks needed to grouped into broad categories. It is likely that risks being reported on the 10-K report will become more specific as the process matures and entities become aware of the number of information security risks they face. When there is more specificity in reporting, this type of study could be conducted with more specific categories.
REFERENCES


APPENDIX A: ADDITIONAL DATA ANALYSIS

Reported risk by type with variance:

<table>
<thead>
<tr>
<th>Year</th>
<th>Configuration</th>
<th>DOS</th>
<th>Hack</th>
<th>Identity Theft</th>
<th>Insider</th>
<th>Maintenance</th>
<th>Malware</th>
<th>Mobile</th>
<th>Phishing</th>
<th>SocialEngineer</th>
<th>ThirdParty</th>
<th>Virus</th>
</tr>
</thead>
<tbody>
<tr>
<td>2007</td>
<td>12</td>
<td>1</td>
<td>7</td>
<td>1</td>
<td>10</td>
<td>18</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>14</td>
<td>10</td>
</tr>
<tr>
<td>2008</td>
<td>14</td>
<td>0</td>
<td>10</td>
<td>2</td>
<td>9</td>
<td>21</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>17</td>
<td>9</td>
</tr>
<tr>
<td>2009</td>
<td>17</td>
<td>0</td>
<td>11</td>
<td>2</td>
<td>11</td>
<td>25</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>19</td>
<td>13</td>
</tr>
<tr>
<td>2010</td>
<td>21%</td>
<td>0%</td>
<td>22%</td>
<td>30%</td>
<td>22%</td>
<td>19%</td>
<td>50%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>12%</td>
<td>4%</td>
</tr>
<tr>
<td>2011</td>
<td>16%</td>
<td>2%</td>
<td>27%</td>
<td>31%</td>
<td>29%</td>
<td>25%</td>
<td>59%</td>
<td>7%</td>
<td>0%</td>
<td>0%</td>
<td>8%</td>
<td>0%</td>
</tr>
<tr>
<td>2012</td>
<td>10%</td>
<td>0%</td>
<td>5%</td>
<td>0%</td>
<td>0%</td>
<td>4%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>2013</td>
<td>9%</td>
<td>0%</td>
<td>9%</td>
<td>22%</td>
<td>0%</td>
<td>5%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>2014</td>
<td>7%</td>
<td>0%</td>
<td>7%</td>
<td>25%</td>
<td>0%</td>
<td>4%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
</tr>
</tbody>
</table>
### Risks by Entity

<table>
<thead>
<tr>
<th>Name</th>
<th>2007</th>
<th>2008</th>
<th>2009</th>
<th>2010</th>
<th>2011</th>
<th>2012</th>
<th>2013</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>Synovus Bank</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>0</td>
<td>7</td>
<td>6</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>JPMorgan Chase Bank, National Association</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>5</td>
<td>9</td>
<td>10</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>Comerica Bank</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>5</td>
<td>5</td>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>Fifth Third Bank</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>6</td>
<td>6</td>
<td>7</td>
<td>7</td>
<td>8</td>
</tr>
<tr>
<td>U.S. Bank National Association</td>
<td>3</td>
<td>3</td>
<td>1</td>
<td>4</td>
<td>4</td>
<td>10</td>
<td>9</td>
<td>9</td>
</tr>
<tr>
<td>Manufacturers and Traders Trust Company</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>3</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>GE Capital Retail Bank</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>3</td>
<td>3</td>
<td>5</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>Ally Bank</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>4</td>
<td>5</td>
<td>9</td>
<td>9</td>
</tr>
<tr>
<td>The Huntington National Bank</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>4</td>
<td>5</td>
<td>5</td>
<td>7</td>
</tr>
<tr>
<td>Bank of America, National Association</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>6</td>
<td>8</td>
<td>9</td>
<td>9</td>
<td>9</td>
</tr>
<tr>
<td>Wells Fargo Bank, National Association</td>
<td>0</td>
<td>0</td>
<td>6</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>7</td>
<td>10</td>
</tr>
<tr>
<td>The Northern Trust Company</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>5</td>
<td>7</td>
<td>8</td>
<td>7</td>
<td>9</td>
</tr>
<tr>
<td>KeyBank National Association</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>8</td>
<td>10</td>
<td>9</td>
<td>9</td>
</tr>
<tr>
<td>Branch Banking and Trust Company</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>11</td>
<td>11</td>
</tr>
<tr>
<td>State Street Bank and Trust Company</td>
<td>3</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>9</td>
<td>9</td>
<td>9</td>
</tr>
<tr>
<td>City National Bank</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>5</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Charles Schwab Bank</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>6</td>
<td>6</td>
<td>11</td>
<td>11</td>
<td>10</td>
</tr>
<tr>
<td>PNC Bank, National Association</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>5</td>
<td>7</td>
<td>8</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>Silicon Valley Bank</td>
<td>3</td>
<td>4</td>
<td>6</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>10</td>
</tr>
<tr>
<td>SunTrust Bank</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>7</td>
<td>5</td>
<td>6</td>
<td>6</td>
<td>8</td>
</tr>
<tr>
<td>Citibank, National Association</td>
<td>5</td>
<td>6</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>8</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>Union Bank, National Association</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>5</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>Goldman Sachs Bank USA</td>
<td>6</td>
<td>6</td>
<td>6</td>
<td>6</td>
<td>8</td>
<td>7</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>Morgan Stanley Bank, National Association</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>8</td>
<td>10</td>
</tr>
<tr>
<td>New York Community Bank</td>
<td>0</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>6</td>
<td>6</td>
<td>6</td>
<td>8</td>
</tr>
<tr>
<td>Hudson City Savings Bank</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>6</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>Capital One, National Association</td>
<td>4</td>
<td>5</td>
<td>4</td>
<td>4</td>
<td>8</td>
<td>7</td>
<td>8</td>
<td>9</td>
</tr>
<tr>
<td>E*TRADE Bank</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>6</td>
<td>6</td>
<td>9</td>
<td>9</td>
</tr>
<tr>
<td>First Niagara Bank, National Association</td>
<td>0</td>
<td>0</td>
<td>6</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>Regions Bank</td>
<td>0</td>
<td>0</td>
<td>6</td>
<td>6</td>
<td>6</td>
<td>8</td>
<td>6</td>
<td>7</td>
</tr>
</tbody>
</table>
### Percentage Matching Risks by Entity

<table>
<thead>
<tr>
<th>Name</th>
<th>2007</th>
<th>2008</th>
<th>2009</th>
<th>2010</th>
<th>2011</th>
<th>2012</th>
<th>2013</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>Synovus Bank</td>
<td>41.67</td>
<td>41.67</td>
<td>41.67</td>
<td>0.00</td>
<td>58.33</td>
<td>50.00</td>
<td>66.67</td>
<td>66.67</td>
</tr>
<tr>
<td>JPMorgan Chase Bank, National Association</td>
<td>33.33</td>
<td>33.33</td>
<td>33.33</td>
<td>41.67</td>
<td>75.00</td>
<td>83.33</td>
<td>83.33</td>
<td>83.33</td>
</tr>
<tr>
<td>Comerica Bank</td>
<td>0.00</td>
<td>16.67</td>
<td>16.67</td>
<td>16.67</td>
<td>41.67</td>
<td>41.67</td>
<td>50.00</td>
<td>50.00</td>
</tr>
<tr>
<td>Fifth Third Bank</td>
<td>33.33</td>
<td>41.67</td>
<td>50.00</td>
<td>50.00</td>
<td>50.00</td>
<td>58.33</td>
<td>58.33</td>
<td>66.67</td>
</tr>
<tr>
<td>U.S. Bank National Association</td>
<td>25.00</td>
<td>25.00</td>
<td>8.33</td>
<td>33.33</td>
<td>33.33</td>
<td>83.33</td>
<td>75.00</td>
<td>75.00</td>
</tr>
<tr>
<td>Manufacturers and Traders Trust Company</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>25.00</td>
<td>25.00</td>
<td>33.33</td>
</tr>
<tr>
<td>GE Capital Retail Bank</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>8.33</td>
<td>25.00</td>
<td>25.00</td>
<td>41.67</td>
<td>33.33</td>
</tr>
<tr>
<td>Ally Bank</td>
<td>16.67</td>
<td>16.67</td>
<td>16.67</td>
<td>33.33</td>
<td>33.33</td>
<td>41.67</td>
<td>75.00</td>
<td>75.00</td>
</tr>
<tr>
<td>The Huntington National Bank</td>
<td>8.33</td>
<td>8.33</td>
<td>8.33</td>
<td>8.33</td>
<td>33.33</td>
<td>41.67</td>
<td>41.67</td>
<td>58.33</td>
</tr>
<tr>
<td>Bank of America, National Association</td>
<td>16.67</td>
<td>16.67</td>
<td>16.67</td>
<td>50.00</td>
<td>66.67</td>
<td>75.00</td>
<td>75.00</td>
<td>75.00</td>
</tr>
<tr>
<td>Wells Fargo Bank, National Association</td>
<td>0.00</td>
<td>0.00</td>
<td>50.00</td>
<td>41.67</td>
<td>50.00</td>
<td>58.33</td>
<td>58.33</td>
<td>50.00</td>
</tr>
<tr>
<td>The Northern Trust Company</td>
<td>33.33</td>
<td>33.33</td>
<td>33.33</td>
<td>41.67</td>
<td>58.33</td>
<td>66.67</td>
<td>58.33</td>
<td>50.00</td>
</tr>
<tr>
<td>KeyBank National Association</td>
<td>25.00</td>
<td>25.00</td>
<td>25.00</td>
<td>25.00</td>
<td>66.67</td>
<td>83.33</td>
<td>75.00</td>
<td>75.00</td>
</tr>
<tr>
<td>Branch Banking and Trust Company</td>
<td>41.67</td>
<td>50.00</td>
<td>58.33</td>
<td>50.00</td>
<td>58.33</td>
<td>66.67</td>
<td>91.67</td>
<td>91.67</td>
</tr>
<tr>
<td>State Street Bank and Trust Company</td>
<td>25.00</td>
<td>25.00</td>
<td>33.33</td>
<td>41.67</td>
<td>50.00</td>
<td>75.00</td>
<td>75.00</td>
<td>75.00</td>
</tr>
<tr>
<td>City National Bank</td>
<td>16.67</td>
<td>16.67</td>
<td>16.67</td>
<td>16.67</td>
<td>33.33</td>
<td>41.67</td>
<td>33.33</td>
<td>33.33</td>
</tr>
<tr>
<td>Charles Schwab Bank</td>
<td>41.67</td>
<td>41.67</td>
<td>41.67</td>
<td>50.00</td>
<td>50.00</td>
<td>91.67</td>
<td>91.67</td>
<td>83.33</td>
</tr>
<tr>
<td>PNC Bank, National Association</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>16.67</td>
<td>41.67</td>
<td>58.33</td>
<td>66.67</td>
<td>66.67</td>
</tr>
<tr>
<td>Silicon Valley Bank</td>
<td>25.00</td>
<td>33.33</td>
<td>50.00</td>
<td>50.00</td>
<td>58.33</td>
<td>66.67</td>
<td>75.00</td>
<td>83.33</td>
</tr>
<tr>
<td>SunTrust Bank</td>
<td>41.67</td>
<td>41.67</td>
<td>41.67</td>
<td>58.33</td>
<td>41.67</td>
<td>50.00</td>
<td>50.00</td>
<td>50.00</td>
</tr>
<tr>
<td>Citibank, National Association</td>
<td>41.67</td>
<td>50.00</td>
<td>50.00</td>
<td>58.33</td>
<td>66.67</td>
<td>66.67</td>
<td>83.33</td>
<td>83.33</td>
</tr>
<tr>
<td>Union Bank, National Association</td>
<td>8.33</td>
<td>16.67</td>
<td>16.67</td>
<td>16.67</td>
<td>33.33</td>
<td>33.33</td>
<td>41.67</td>
<td>41.67</td>
</tr>
<tr>
<td>Goldman Sachs Bank USA</td>
<td>50.00</td>
<td>50.00</td>
<td>50.00</td>
<td>50.00</td>
<td>50.00</td>
<td>66.67</td>
<td>58.33</td>
<td>66.67</td>
</tr>
<tr>
<td>Morgan Stanley Bank, National Association</td>
<td>16.67</td>
<td>16.67</td>
<td>16.67</td>
<td>33.33</td>
<td>41.67</td>
<td>50.00</td>
<td>66.67</td>
<td>83.33</td>
</tr>
<tr>
<td>New York Community Bank</td>
<td>0.00</td>
<td>25.00</td>
<td>25.00</td>
<td>25.00</td>
<td>50.00</td>
<td>50.00</td>
<td>50.00</td>
<td>50.00</td>
</tr>
<tr>
<td>Hudson City Savings Bank</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>50.00</td>
<td>66.67</td>
<td>66.67</td>
</tr>
<tr>
<td>Capital One, National Association</td>
<td>33.33</td>
<td>41.67</td>
<td>33.33</td>
<td>33.33</td>
<td>66.67</td>
<td>58.33</td>
<td>66.67</td>
<td>75.00</td>
</tr>
<tr>
<td>E*TRADE Bank</td>
<td>41.67</td>
<td>41.67</td>
<td>41.67</td>
<td>41.67</td>
<td>50.00</td>
<td>50.00</td>
<td>75.00</td>
<td>75.00</td>
</tr>
<tr>
<td>First Niagara Bank, National Association</td>
<td>0.00</td>
<td>0.00</td>
<td>50.00</td>
<td>41.67</td>
<td>50.00</td>
<td>58.33</td>
<td>58.33</td>
<td>58.33</td>
</tr>
<tr>
<td>Regions Bank</td>
<td>0.00</td>
<td>0.00</td>
<td>50.00</td>
<td>50.00</td>
<td>50.00</td>
<td>66.67</td>
<td>50.00</td>
<td>58.33</td>
</tr>
</tbody>
</table>
Graphical view of proposed project

1. **10-K Cybersecurity Risk Reports**
   - Yearly 2007 - 2013
   - 100 largest US Banks by Deposits

2. **8-K Material Incident Reports**

3. **Categorize Data with Codebook**

4. **Quantitative Data to Database**

5. **10-K Financial Performance Reports**

6. **HP Threat Report**

7. **Symantec Threat Report**

8. **SANS Data**

9. **Categorize Data with Codebook**

10. **Determine Convergence**

   - Convergence will be tested until it is deemed impossible. At that point data will be evaluated separately.

11. **Data matched Risk/Threat by year**

12. **Report: Guidance**

13. **Report: Maturity**


15. **Report: Realization**
## APPENDIX C: CODING CATALOG

<table>
<thead>
<tr>
<th>10-K expression</th>
<th>Threat Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account takeovers</td>
<td>Identity theft</td>
</tr>
<tr>
<td>Breach</td>
<td>Hack</td>
</tr>
<tr>
<td>Cyber Attacks</td>
<td>Hack</td>
</tr>
<tr>
<td>Degradation of service</td>
<td>DOS</td>
</tr>
<tr>
<td>e-Fraud</td>
<td>Identity theft</td>
</tr>
<tr>
<td>Electrical Outage</td>
<td>Not included. This is a business continuation issue</td>
</tr>
<tr>
<td>Employee Tampering</td>
<td>Insider</td>
</tr>
<tr>
<td>Employee tampering</td>
<td>Insider</td>
</tr>
<tr>
<td>Faulty or failed equipment</td>
<td>Maintenance</td>
</tr>
<tr>
<td>improper implementation of systems</td>
<td>Configuration</td>
</tr>
<tr>
<td>Improper use of system</td>
<td>Hack</td>
</tr>
<tr>
<td>improve system failure</td>
<td>Configuration</td>
</tr>
<tr>
<td>Inadequate Systems</td>
<td>Configuration</td>
</tr>
<tr>
<td>Induce frequently information</td>
<td>Social Engineering</td>
</tr>
<tr>
<td>Intercepted Data</td>
<td>Hack</td>
</tr>
<tr>
<td>Internal Security Breach</td>
<td>Insider</td>
</tr>
<tr>
<td>Interruption</td>
<td>Not included. Just stating an interruption in system functions is not specific enough to include.</td>
</tr>
<tr>
<td>Malfeasance</td>
<td>Insider</td>
</tr>
<tr>
<td>Malfunction</td>
<td>Maintenance</td>
</tr>
<tr>
<td>Natural Disaster</td>
<td>Not included. Natural disasters are a business continuation issue</td>
</tr>
<tr>
<td>Outsourced Vendors</td>
<td>Third-party</td>
</tr>
<tr>
<td>Overloaded System</td>
<td>Configuration</td>
</tr>
<tr>
<td>Programming Error</td>
<td>Configuration</td>
</tr>
<tr>
<td>Shortcoming of System</td>
<td>Configuration</td>
</tr>
<tr>
<td>Spam Attack</td>
<td>Phishing</td>
</tr>
<tr>
<td>System flaws</td>
<td>Configuration</td>
</tr>
<tr>
<td>System Flaws</td>
<td>Configuration</td>
</tr>
<tr>
<td>Systems inability to act correctly in normal operation.</td>
<td>Configuration</td>
</tr>
<tr>
<td>Targeted Attacks</td>
<td>Hack</td>
</tr>
<tr>
<td>10-K expression</td>
<td>Threat Name</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Technical Flaws</td>
<td>Configuration</td>
</tr>
<tr>
<td>Terrorism</td>
<td>Not included. The term is too generic. If they describe a security threat that terrorism causes then it will be included</td>
</tr>
<tr>
<td>Transaction volume increase failed system</td>
<td>Configuration</td>
</tr>
<tr>
<td>Unauthorized Access to System</td>
<td>Hack</td>
</tr>
<tr>
<td>Unavailable online banking system</td>
<td>DOS</td>
</tr>
<tr>
<td>Unlawful Tampering</td>
<td>Hack</td>
</tr>
</tbody>
</table>
APPENDIX D: SCATTER DIAGRAMS
APPENDIX E: CF DISCLOSURE GUIDANCE NO. 2

Division of Corporation Finance
Securities and Exchange Commission

CF Disclosure Guidance: Topic No. 2

Cybersecurity

**Date:** October 13, 2011

**Summary:** This guidance provides the Division of Corporation Finance's views regarding disclosure obligations relating to cybersecurity risks and cyber incidents.

**Supplementary Information:** The statements in this CF Disclosure Guidance represent the views of the Division of Corporation Finance. This guidance is not a rule, regulation, or statement of the Securities and Exchange Commission. Further, the Commission has neither approved nor disapproved its content.

Introduction

For a number of years, registrants have migrated toward increasing dependence on digital technologies to conduct their operations. As this dependence has increased, the risks to registrants associated with cybersecurity have also increased, resulting in more frequent and severe cyber incidents. Recently, there has been increased focus by registrants and members of the legal and accounting professions on how these risks and their related impact on the operations of a registrant should be described within the framework of the disclosure obligations imposed by the federal securities laws. As a result, we determined that it would be beneficial to provide guidance that assists registrants in assessing what, if any, disclosures should be provided about cybersecurity matters in light of each registrant’s specific facts and circumstances.

We prepared this guidance to be consistent with the relevant disclosure considerations that arise in connection with any business risk. We are mindful of potential concerns that detailed disclosures could compromise cybersecurity efforts -- for example, by providing a “roadmap” for those who seek to infiltrate a registrant’s network security -- and we emphasize that disclosures of that nature are not required under the federal securities laws.
In general, cyber incidents can result from deliberate attacks or unintentional events. We have observed an increased level of attention focused on cyber attacks that include, but are not limited to, gaining unauthorized access to digital systems for purposes of misappropriating assets or sensitive information, corrupting data, or causing operational disruption. Cyber attacks may also be carried out in a manner that does not require gaining unauthorized access, such as by causing denial-of-service attacks on websites. Cyber attacks may be carried out by third parties or insiders using techniques that range from highly sophisticated efforts to electronically circumvent network security or overwhelm websites to more traditional intelligence gathering and social engineering aimed at obtaining information necessary to gain access.

The objectives of cyber attacks vary widely and may include theft of financial assets, intellectual property, or other sensitive information belonging to registrants, their customers, or other business partners. Cyber attacks may also be directed at disrupting the operations of registrants or their business partners. Registrants that fall victim to successful cyber attacks may incur substantial costs and suffer other negative consequences, which may include, but are not limited to:

- Remediation costs that may include liability for stolen assets or information and repairing system damage that may have been caused. Remediation costs may also include incentives offered to customers or other business partners in an effort to maintain the business relationships after an attack;
- Increased cybersecurity protection costs that may include organizational changes, deploying additional personnel and protection technologies, training employees, and engaging third party experts and consultants;
- Lost revenues resulting from unauthorized use of proprietary information or the failure to retain or attract customers following an attack;
- Litigation; and
- Reputational damage adversely affecting customer or investor confidence.

Disclosure by Public Companies Regarding Cybersecurity Risks and Cyber Incidents

The federal securities laws, in part, are designed to elicit disclosure of timely, comprehensive, and accurate information about risks and events that a reasonable investor would consider important to an investment decision. Although no existing disclosure requirement explicitly refers to cybersecurity risks and cyber incidents, a number of disclosure requirements may impose an obligation on registrants to disclose such risks and incidents. In addition, material information regarding cybersecurity risks and cyber incidents is required to be disclosed when necessary in order to make other required disclosures, in light of the circumstances under which they are made, not misleading. Therefore, as with other operational and financial risks, registrants should
review, on an ongoing basis, the adequacy of their disclosure relating to cybersecurity risks and cyber incidents.

The following sections provide an overview of specific disclosure obligations that may require a discussion of cybersecurity risks and cyber incidents.

Risk Factors

Registrants should disclose the risk of cyber incidents if these issues are among the most significant factors that make an investment in the company speculative or risky. In determining whether risk factor disclosure is required, we expect registrants to evaluate their cybersecurity risks and take into account all available relevant information, including prior cyber incidents and the severity and frequency of those incidents. As part of this evaluation, registrants should consider the probability of cyber incidents occurring and the quantitative and qualitative magnitude of those risks, including the potential costs and other consequences resulting from misappropriation of assets or sensitive information, corruption of data or operational disruption. In evaluating whether risk factor disclosure should be provided, registrants should also consider the adequacy of preventative actions taken to reduce cybersecurity risks in the context of the industry in which they operate and risks to that security, including threatened attacks of which they are aware.

Consistent with the Regulation S-K Item 503(c) requirements for risk factor disclosures generally, cybersecurity risk disclosure provided must adequately describe the nature of the material risks and specify how each risk affects the registrant. Registrants should not present risks that could apply to any issuer or any offering and should avoid generic risk factor disclosure. Depending on the registrant’s particular facts and circumstances, and to the extent material, appropriate disclosures may include:

- Discussion of aspects of the registrant’s business or operations that give rise to material cybersecurity risks and the potential costs and consequences;
- To the extent the registrant outsources functions that have material cybersecurity risks, description of those functions and how the registrant addresses those risks;
- Description of cyber incidents experienced by the registrant that are individually, or in the aggregate, material, including a description of the costs and other consequences;
- Risks related to cyber incidents that may remain undetected for an extended period; and
- Description of relevant insurance coverage.

A registrant may need to disclose known or threatened cyber incidents to place the discussion of cybersecurity risks in context. For example, if a registrant experienced a
material cyber attack in which malware was embedded in its systems and customer data was compromised, it likely would not be sufficient for the registrant to disclose that there is a risk that such an attack may occur. Instead, as part of a broader discussion of malware or other similar attacks that pose a particular risk, the registrant may need to discuss the occurrence of the specific attack and its known and potential costs and other consequences.

While registrants should provide disclosure tailored to their particular circumstances and avoid generic “boilerplate” disclosure, we reiterate that the federal securities laws do not require disclosure that itself would compromise a registrant’s cybersecurity. Instead, registrants should provide sufficient disclosure to allow investors to appreciate the nature of the risks faced by the particular registrant in a manner that would not have that consequence.

---

### Endnotes


2. The information in this disclosure guidance is intended to assist registrants in preparing disclosure required in registration statements under the Securities Act of 1933 and periodic reports under the Securities Exchange Act of 1934. In order to maintain the accuracy and completeness of information in effective shelf registration statements, registrants may also need to consider whether it is necessary to file reports on Form 6-K or Form 8-K to disclose the costs and other consequences of material cyber incidents. See Item 5(a) of Form F-3 and Item 11(a) of Form S-3.

3. Securities Act Rule 408, Exchange Act Rule 12b-20, and Exchange Act Rule 14a-9. Information is considered material if there is a substantial likelihood that a reasonable investor would consider it important in making an investment decision or if the information would significantly alter the total mix of information made available. See Basic Inc. v. Levinson, 485 U.S. 224 (1988); and TSC Industries, Inc. v. Northway, Inc., 426 U.S. 438 (1976). Registrants also should consider the antifraud provisions of the federal securities laws, which apply to statements and omissions both inside and outside
of Commission filings. See Securities Act Section 17(a); Exchange Act Section 10(b); and Exchange Act Rule 10b-5.

4 See Item 503(c) of Regulation S-K; and Form 20-F, Item 3.D.

5 Item 503(c) of Regulation S-K instructs registrants to “not present risks that could apply to any issuer or any offering” and further, to “[e]xplain how the risk affects the issuer or the securities being offered.” Item 503(c) of Regulation S-K.
APPENDIX F: SEC ANTICDOTAL DATA

Google

In January 2010, Google made news when it disclosed that hackers based in China had raided the company’s networks. It reported that breach to the SEC in a —Current Report (Form 8-K) filed in January 2010, well before CF DG 2 was issued. The Annual Report the company issued in January 2012 made only tentative statements about cybersecurity, referencing (as had the other companies here reviewed) what would happen —[i]f our security measures are breached. The SEC invoked CF DG 2 when asking Google to revise its disclosure to reference the 2010 attack —to provide the proper context for your risk factor disclosures. Google agreed, and in its subsequent disclosures, it noted that it —experience[s] cyber-attacks of varying degrees on a regular basis, and . . . unauthorized parties have obtained, and may in the future obtain, access to our data . . . [possibly resulting in] an adverse effect on our business.

Foot Notes:

Amazon.com

A leader in Internet retail, Amazon.com has a market capitalization of about $170 billion, 117,000 employees, and 2012 revenues of over $60 billion. The online shoe portal Zappos.com—dubbed a “shoe utopia” by the press—is a subsidiary of Amazon’s. Recently, there was trouble in paradise: in January 2012, an unknown perpetrator infiltrated Zappos’ internal computer network through servers housed in Shepherdsville, Kentucky and may have had —illegal and unauthorized access— to customer account information, including customers’ names, e-mail addresses, billing and shipping addresses, phone numbers, the last four digits of their credit card numbers, and their —cryptographically scrambled password[s]. The episode garnered significant press and spurred class action suits for a litany of civil wrongs.

A few weeks later, Amazon filed its standard Annual Report (Form 10-K) with the SEC. It made only vague references to the potential of cyber intrusions that —could expose us or our customers to a risk of loss or misuse of [personal] information, adversely affect our operating results, result in litigation or potential liability for us and otherwise harm our business. The report made no mention of the intrusion that had just occurred and triggered lawsuits.

The SEC replied to Amazon’s Annual Report and cited the recent news that, far from a mere hypothetical intrusion, a cyber-attack on its Zappos subsidiary had —occurred during which millions of user accounts were compromised; accordingly, it asked the company to —please address whether disclosure in its 10-K of such an attack was necessary to advise possible investors of all potential harm to its business, including —reputational damage affecting customer or investor confidence. To support its request for greater disclosure, the SEC cited CF DG 2.

At first Amazon protested, claiming that —information on the specific incident would not provide investors with additional material information relating to the cyber-attack risks facing our business, that the attack had no material impact on Amazon, and that any impact on Zappos would be —transitory. Undeterred, the SEC again pressed Amazon to —expand its 10-K —to disclose that you have experienced cyber-attacks and breaches in a second letter the following month. This time, Amazon obliged. It wrote in its next filing that some of its subsidiaries —had past security breaches, and, although they did not have a
material adverse effect on our operating results, there can be no assurance of a similar result in the future.\footnote{187} It is unclear what effect, if any, Amazon’s subtle word change had on shareholders’ investment decisions.

Foot Notes:
\footnote{179}Alexandra Jacobs, Happy Feet, NEW YORKER, SEPT. 14, 2009, at 66.
\footnote{180}Tony Hsieh, Security Email, ZAPPOS.COM (Jan. 15, 2012), http://blogs.zappos.com/securityemail (explaining cyberattack and company’s immediate remediation measures to employees, including the email subsequently sent to customers).
\footnote{182}Amazon.com, Inc., Annual Report (Form 10-K), at 10 (Feb. 1, 2012) (emphasis added).
\footnote{184}Id. (―Please tell us what consideration you gave to including expanded disclosure consistent with the guidance provided by the Division of Corporation Finance’s Disclosure Guidance Topic No. 2.‖).
\footnote{187}Amazon.com, Inc., Quarterly Report (Form 10-Q), at 34 (July 27, 2012).
APPENDIX G: SEC REGULATION S-K 229.503 (C)

229.503 (Item 503) Prospectus summary, risk factors, and ratio of earnings to fixed charges. The registrant must furnish this information in plain English. See § 230.421(d) of Regulation C of this chapter.

(a) Prospectus summary. Provide a summary of the information in the prospectus where the length or complexity of the prospectus makes a summary useful. The summary should be brief. The summary should not contain, and is not required to contain, all of the detailed information in the prospectus. If you provide summary business or financial information, even if you do not caption it as a summary, you still must provide that information in plain English.

Instruction to paragraph 503(a): The summary should not merely repeat the text of the prospectus but should provide a brief overview of the key aspects of the offering. Carefully consider and identify those aspects of the offering that are the most significant and determine how best to highlight those points in clear, plain language.

(b) Address and telephone number. Include, either on the cover page or in the summary section of the prospectus, the complete mailing address and telephone number of your principal executive offices.

(c) Risk factors. Where appropriate, provide under the caption “Risk Factors” a discussion of the most significant factors that make the offering speculative or risky. This discussion must be concise and organized logically. Do not present risks that could apply to any issuer or any offering. Explain how the risk affects the issuer or the securities being offered. Set forth each risk factor under a subcaption that adequately describes the risk. The risk factor discussion must immediately follow the summary section. If you do not include a summary section, the risk factor section must immediately follow the cover page of the prospectus or the pricing information section that immediately follows the cover page. Pricing information means price and price-related information that you may omit from the prospectus in an effective registration statement based on § 230.430A(a) of this chapter. The risk factors may include, among other things, the following:

1. Your lack of an operating history;
2. Your lack of profitable operations in recent periods;
3. Your financial position;
4. Your business or proposed business; or
5. The lack of a market for your...
common equity securities or securities convertible into or exercisable for common equity securities.

(d) Ratio of earnings to fixed charges. If you register debt securities, show a ratio of earnings to fixed charges. If you register preference equity securities, show the ratio of combined fixed charges and preference dividends to earnings. Present the ratio for each of the last five fiscal years and the latest interim period for which financial statements are presented in the document.

If you will use the proceeds from the sale of debt or preference securities to repay any of your outstanding debt or to retire other securities and the change in the ratio would be ten percent or greater, you must include a ratio showing the application of the proceeds, commonly referred to as the pro forma ratio.

Instructions to paragraph 503(d): 1. Definitions.

In calculating the ratio of earnings to fixed charges, you must use the following definitions:

(A) Fixed charges. The term “fixed charges” means the sum of the following: (a) interest expensed and capitalized, (b) amortized premiums, discounts and capitalized expenses related to indebtedness, (c) an estimate of the interest within rental expense, and (d) preference security dividend requirements of consolidated subsidiaries.

(B) Preference security dividend. The term “preference security dividend” is the amount of pre-tax earnings that is required to pay the dividends on outstanding preference securities. The dividend requirement must be computed as the amount of the dividend divided by (1 minus the effective income tax rate applicable to continuing operations).

(C) Earnings. The term “earnings” is the amount resulting from adding and subtracting the following items. Add the following: (a) pre-tax income from continuing operations before adjustment for income or loss from equity investees; (b) fixed charges; (c) amortization of capitalized interest; (d) distributed income of equity investees; and (e) your share of pre-tax losses of equity investees for which charges arising from guarantees are included in fixed charges. From the total of the added items, subtract the following: (a) interest capitalized; (b) preference security dividend requirements of consolidated subsidiaries; and (c) the noncontrolling interest in pre-tax income of subsidiaries that have not incurred fixed charges. Equity investees are investments that you account for using the equity method of accounting. Public utilities following
SFAS 71 should not add amortization of capitalized interest in determining earnings, nor reduce fixed charges by any allowance for funds used during construction.

2. Disclosure. Disclose the following information when showing the ratio of earnings to fixed charges:

(A) Deficiency. If a ratio indicates less than one-to-one coverage, disclose the dollar amount of the deficiency.

(B) Pro forma ratio. You may show the pro forma ratio only for the most recent fiscal year and the latest interim period. Use the net change in interest or dividends from the refinancing to calculate the pro forma ratio.

(C) Foreign private issuers. A foreign private issuer must show the ratio based on the figures in the primary financial statement. A foreign private issuer must show the ratio based on the figures resulting from the reconciliation to U.S. generally accepted accounting principles if this ratio is materially different.

(D) Summary Section. If you provide a summary or similar section in the prospectus, show the ratios in that section.

3. Exhibit. File an exhibit to the registration statement to show the figures used to calculate the ratios. See paragraph (b)(12) of Item 601 of Regulation S-K (17 CFR 229.601(b)(12)).

(e) Smaller reporting companies. A registrant that qualifies as a smaller reporting company, as defined by § 229.10(f), need not comply with paragraph (d) of this Item.

Instruction to Item 503: For asset-backed securities, see also Item 1103 of Regulation AB (§ 229.1103).