Accuracy of Self Disclosed Cybersecurity Risks of Large U.S. Banks

Troy G. Bakker
Dakota State University

Kevin Streff
Dakota State University

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.

BACKGROUND OF THE PROBLEM

The United States' securities markets have been touted as the most financially transparent markets in the world. This fiscal transparency is manifest in the accessibility and quality of financial information available to investors (Williams, 1999). Investors utilize this data 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 over 50% of U.S. households invest in corporate stocks and bonds, directly or indirectly, through pension plans, mutual funds, or employee stock ownership plans. (Saad, 2013).

While investor intent and knowledge may differ, one constant holds true: 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 mandate of accessible high-quality data, in 2005 the SEC began requesting that corporations include material risk information on their mandated reports (SEC, 2005). In 2011, this request began calling for cybersecurity risks information to be included (Ferro, 2013). Corporations disclose this risk data on an SEC report known as the 10-K report. The self-disclosed cybersecurity data communicates the cybersecurity risks that a corporation faces in day-to-day operation. The reported information is used by the investing public to determine if they are willing to invest in an organization with specific risks that may diminish corporate value.

One does not have to look very far to see how a cybersecurity breach can affect a corporation's value. The large international retailer, Target Corporation, was the victim of a massive cybersecurity breach in late 2013. The records of some 100 million customers were affected by the breach. The attack precipitated a substantial drop in Target's earnings for the 2013 fourth quarter of nearly 50%. Litigation against the company continues; ongoing costs are unknown.

Additionally, the retailer's stock lost approximately 9% of its value. Expenses associated with the breach in 2013 were over $66 million (McGrath, 2014). A study by Acquisti et al. indicates that stock price devaluation precipitated by a security breach is temporary in nature most stocks return to their previous level within a fairly short amount of time (Acquisti et al, 2006). This appears to be true with the Target breach as well. Target's stock price returned to its pre-breach price by November 2014. However, the Acquisti et al. study does not take into account the stock price appreciation of competitors for the period. Walmart Corporation, one of Target's chief competitors, realized stock appreciation up to 15% percent above Target.

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 likely lost stock price appreciation of $2 - 6 billion for almost all of 2014.

As indicated, the effect of the breach to the shareholder was significant. But, shareholders were unaware of the existing cybersecurity risk. The breach was the result of malware installed on Target's point-of-sale system. However, Target's 2012 10-K report did not list malware as a risk to the company. Furthermore, Target does talk of the risk of a data breach but does not elaborate as to the possible vector of a breach. Therefore, the investors were not informed that malware was a potential threat for Target. Protecting the investing public from this type of information deficiency is the primary goal of the SEC, and the 10-K report is its reporting mechanism. The Target example demonstrates why the SEC has heightened its concern of cybersecurity risk issues.

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

As events similar to the Target breach affect more and more households, consumer visibility of such issues has also increased. 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 (Ferro, 2013). This communication compelled the SEC to issue a guideline instructing corporations how to complete the cybersecurity risk section of the 10-K report. The SEC had hoped that additional guidance would increase the accuracy of the self-disclosed data.

This SEC guideline has been criticized as being vague and its effectiveness has been repeatedly questioned. However, the SEC countered these ineffectiveness claims with anecdotal data touting the successes of the guideline (Ferro, 2013). While the subjective data appears encouraging, there has not been an analytical study to validate the SEC's claims of success. This current study will be the first scientific study to examine the accuracy of cybersecurity risk reporting and factors that affect reporting accuracy.

STATEMENT OF THE PROBLEM

Publicly traded corporations must supply the SEC with data regarding their information-security risks. The data is included on the mandatory reports uploaded to the SEC's online system. This mandatory information is used by investors to help determine the fair market value of a corporation's stock. Unlike financial data, data on 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 threats they face. These inaccuracies can result in an inflated stock price and a reduced understanding of the corporation's true information-security risks.

OBJECTIVES

Along with determining accuracy, this project presents and evaluates a model that hypothesizes the factors that determine the accuracy of information-security-risk reporting. The project hypothesizes that Guidance, Maturity, Performance, and Realization are factors that influence reporting accuracy. These variables are defined below:

1. Lack of guidance about 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 that a particular threat is present in the industry (Realization)

The first task in this study was to quantify the disparity of reported cybersecurity risks and industry threats. This was accomplished by taking a sample of the self-disclosed, cybersecurity risk data of publicly traded corporate banks. The data was then compared to threat data. The threat data consists of the cybersecurity risks reported by the entire sample population. The threat categories were then reviewed and distilled into 12 general categories.

Differences between self-disclosed risk and threats reveal deficiencies in the self-disclosure process. The study then compares the risk disclosure disparity over several years. The level of disparity is expected to fluctuate throughout the years as events related to the hypothesized factors occur. Analysis of disparity will delineate the hypothesized factors for the model.

LITERATURE REVIEW

This study examined qualitative data on self-disclosed cybersecurity risks as collected by the SEC. Unlike financial data provided to shareholders, cybersecurity risks are unaudited (IAS Plus, 2014). The shareholder is therefore relying on the reporting corporation to ensure the data are correct. This study will determine if cybersecurity risk data reported by large U.S. banks are in step within industry threat data. To that end, this literature review will examine the following topics using the body of knowledge base in the information assurance domain.

1. Brief history of SEC reporting
2. Studies similar to this study
3. Other studies using SEC mandatory reports

After the stock market crash of 1929, the United States found its previously robust economy struggling and the stock market falling (Keller, 1988). When the market slide abated, public corporations lost 83% of their value. The stock market would not return to pre-1929 levels until the mid-1950's (Bhide, 1991).

Following the stock market crash, the world found that it was in the midst of the Great Depression. Although the U.S. had dealt with many other economic downturns, this was to date the worst in history. Determining that the stock market crash was a major contributor to the Great Depression, Congress enacted the Securities and Exchange Acts in 1933 and 1934. The acts were intended to prevent any future stock market calamities. The Securities and Exchange Acts effectively moved the oversight of publicly-traded corporations from individual states to the federal government. This transfer of regulating authority facilitated the creation of the SEC (Macey & Miller, 1991).

One of the primary objectives of the newly created SEC was to protect investors by ensuring they have the same accurate financial information as a corporation's management (Bhide, 1991; SEC, 2014). Currently, cybersecurity risk information is collected on SEC mandated 10-K and 10-Q reports (10-K is yearly and 10-Q quarterly) which are available to the general public.

Given the scarcity of like projects, this study will examine closely related ventures with the hopes of drawing a parallel with other self-disclosed risk studies. Although the SEC requested cybersecurity risk data in 2009, 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 operational risk (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 as if the reliability of this index is maturing as banks become more educated in 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 manifest 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.

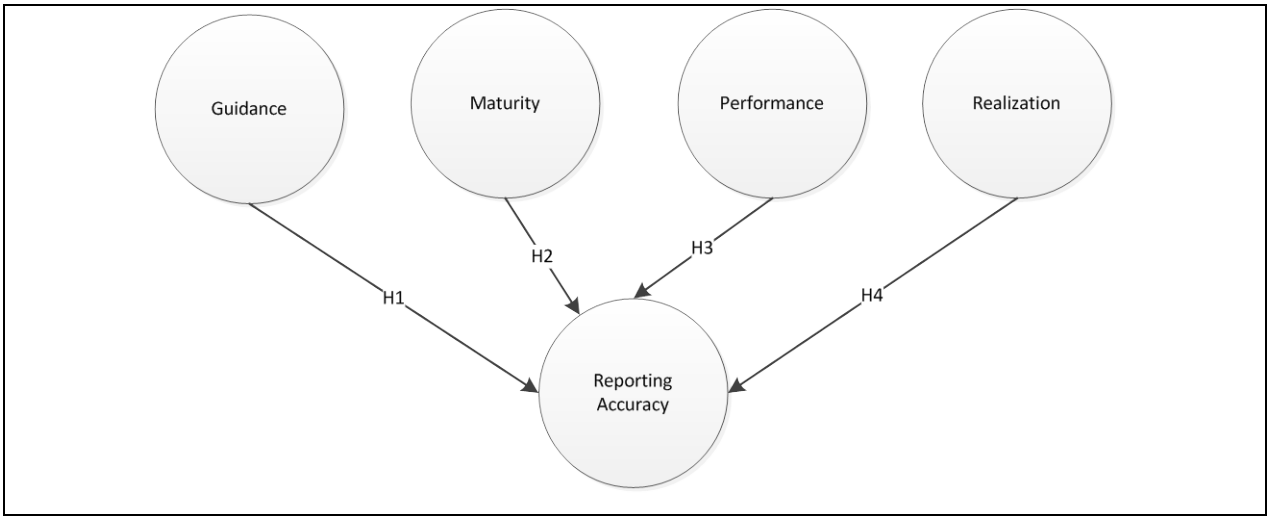
Other studies have utilized self-disclosed cybersecurity risk as an indicator of a potential data breach (Wang, Kannan, & Ulmer, 2013) or perception of risk (Campbell, Chen, Dhaliwal, Lu & Steele, 2011) but none compared the data to the reported threats. Furthermore, previous studies have not been conducted using data collected after the 2011 SEC guideline was published.

As presented in this brief 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 for the first time information security risk. It will add to the body of knowledge as no other study has been carried out after the SEC request for cybersecurity risk data and its 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 will be compared to industry recognized threats.

RESEARCH MODEL

Beyond determining the accuracy of cybersecurity risks reporting, the goal of the data analysis is 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 1.

FIGURE 1
PROJECT MODEL



Each association with the reporting accuracy construct represents a hypothesized relation between the two constructs. The hypotheses are presented below;

1. H1: Guidance contributes to Reporting Accuracy
2. H2: Maturity does occur and contributes to Reporting Accuracy
3. H3: Profitable corporations have higher Reporting Accuracy
4. H4: A cybersecurity incident will increase Reporting Accuracy

THEORETICAL FOUNDATION

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

Lack of Guidance

The theoretical basis for the lack of guidance cause and effect relationship is the general deterrence theory (GDT). The GDT states that the perceived likelihood of being caught and the perceived severity of punishment are key decision factors as one considers committing an infraction (Gibbs, 1975). In this model the infraction is intentionally underreporting cybersecurity risk. The punishment would be some legal action initiated from 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. When the cybersecurity risk reporting guideline was published in 2011 it, in effect, informed corporations that cybersecurity risks are material risks. Therefore, not correctly reporting cybersecurity risk violates an SEC directive. The study treats the SEC request for accurate risk reporting as a law and not doing so an infraction of that law. This treatment of the SEC guideline as law makes the General Deterrence Theory an appropriate basis for the study. If the GDT applies to this situation, there will be an observable increase in reporting accuracy after the 2011 guideline publication. This increase in accuracy would be due to the corporations attempt to comply with the SEC's request.

Gaining Experience

Maturity, in the context of this study referrers 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 predominately used in a 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, an analysis will show that reporting becomes more accurate as corporations gain experience. In the 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.

Intentional Underreporting

The Securities and Exchange Commission receives its authority from two acts passed by congress in 1933 and 1934. The acts are general in nature but do stress the importance of transparency between the corporations and shareholders. The intent is 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, researchers observed that corporate managers delay sharing bad news to investors (Kothari et al., 2009). While other studies have found no evidence that risk disclosure is related to financial performance (Linsley, Shrives & Crumpton, 2006), the study used general disclosure statements to base their conclusion. This study will concentrate on information security risk statements to determine if the agency theory phenomenon is occurring.

Awareness of Risk

Although corporations should be aware of the cybersecurity risks that are present within their corporate domain, it is possible they underreport risks out of unawareness. They may believe that a threat does not apply or they have no exposure. They also may wish to avoid detailing the risk to their stockholders for self-serving purposes as described by the 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 that the corporation will attempt to limit their liability by being vigilant in correctly reporting all risks (Skinner, 1994). The General Deterrent Theory would also be valid as the corporation attempt 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.

RESEARCH METHODOLOGY

The primary data collection methodology used for this thesis was qualitative data analysis because it uses textual reports to derive data. The textual data was then transformed to quantitative data by coding the data into generalized classifications. This quantitative data was then used for all data analysis.

The study used a sample of the 30 largest commercial banks in the United States. The final year-end 10-K reports for these 30 banks from 2007 to 2014 were obtained from the SEC. 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 was a qualitative codebook which 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 were compared to the threat information collected inductively from

the 10-K reports. All matches were recorded in a database. 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. Then suppose that the threat data indicated that there were 15 threat categories. This would then give ABC Bank a matching total of .4 ($\sum$ risk / 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 same technique was used by researchers to examine the accuracy of self-disclosed material risks (Campbell, Chen, Dhaliwal, Lu, & Steele, 2011). This technique was also employed in a study attempting 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 one and losses as a zero.

It was also necessary to capture if 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. Also, 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.

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 product named Stata which is a commercially available statistical analysis package from Stat corp. This product was chosen primarily for its ability to easily analyze panel data and it also has a large user community and a support staff to help with technical or analytical issues. Although several regression analysis techniques were considered, panel data analysis with fixed effect was the most appropriate methodology. This method was chosen because there is longitudinal data for each entity and the focus in on variables across time. Panel data analysis works effectively for this type of analysis insofar as 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. This test determines if the unique error is correlated with the regressor (Greene, 2009). If the error is correlated, the random and or single level mixed method of analysis may be more appropriate form of analysis than the fixed method. The results of the Hausman test indicate little difference in the coefficients from the fixed and random analysis methods. Furthermore, there was a high degree of significance as the value of chi-squared was 0.9942 indicating that the fixed effects model is appropriate.

The dataset was also tested for autocorrelation using the Woodridge test. Since the outcome of the test is insignificant, it indicates there is no autocorrelation effect. The data was also tested for heterogeneity. Analysis of the data indicates that are considerable differences in the mean of the dependent variable resulting in an upward progression. This result is indicative of the effect of the maturity and guidance variable.

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 illicit the recognition of a risk. 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.

In this study, the threats within the domain of the study were assigned a category name. Therefore, an unmatched threat represented a risk that an entity had not disclosed to their stockholders. Examining the percentage of self-disclosed risks to threats give us an idea of how accurate an entity self-disclosed risk reporting is on their 10-K reports. To this end, the study examines 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:

$$\frac{\sum \text{Reported Risks}}{\sum \text{All Categories}} \quad (1)$$

The percentages for each entity were then averaged and sorted by year. The average matching percentages of the 30 entities is 20.56%. Therefore, of the 12 risk categories included in this study, only two or three are reported. This percentage increases progressively through the years until 2014 where an average 66.67% of risks are self-disclosed. Furthermore, the standard deviation has decreased from 16.77 to 15.81 indicating there is less variance in each entities matching percentage.

Analysis of the matching percentage indicates that entities are now reporting more information security risks than previous years. It also looks as if a larger number of entities are reporting an increased amount of risk. While this is indeed encouraging, the numbers also indicate that companies are still underreporting information security risks by 33% or approximately four risk categories. Although the number of reported risks is 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 has begun as early as 2007 and has continued to a lessening degree through all eight years of the study. The analysis of the data further demonstrates that none of the study subject entities reported 100% of the risk categories on their 10-K reports. The entities highest percentages of reported risks in 2014 were 92% and 83%.

Maturity Analysis

The 10-K report data being analyzed for this study spanned eight years from 2007 through 2014. During this time it is likely that those creating the 10-K reports have become 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 samples is to calculate the variance of cumulative matching percentage from year to year. The calculation for this variance is as follows:

$$\frac{\sum \text{Risks}_{\text{Year 2}} - \sum \text{Risks}_{\text{Year 1}}}{\sum \text{Risks}_{\text{Year 1}}} \quad (2)$$

Table 1: represents the variance for each year of the study data. As indicated by the data, each year we see a positive increase in variance thus representing an increase in the number of cumulative risks being reported. Between 2007 and 2008 there was an increase in reported risks of 15%. The final year of data, 2014 realizes an increase of 7% over the previous year.

TABLE 1
CUMULATIVE MATCHING VARIANCE

	2007	2008	% Var	2009	% Var	2010	% Var	2011	% Var	2012	% Var	2013	% Var	2014	% Var
Total Matching	74	85	15%	105	24%	118	12%	166	41%	202	22%	224	11%	240	7%

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 regression analysis techniques were enlisted. 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 Table 2:

TABLE 2
REGRESSION ANALYSIS

match	Coef.	Std. Err.	t	P>|t|	[95% Conf.	Interval]
eps_ind	.6621188	2.434709	0.27	0.786	-4.137887	5.462124
mat_1	5.505518	.640896	8.59	0.000	4.241997	6.769038
guide	9.112059	2.978983	3.06	0.003	3.239022	14.9851
_cons	12.26739	2.666955	4.60	0.000	7.009518	17.52527
sigma_u	14.35803					
sigma_e	11.095081					
rho	.62612187	(fraction of variance due to u_i)				

In table 2: the independent variables guidance, maturity and performance are labeled as guide, mat_1, eps_ind, respectively. The fixed effects panel data regression calculation for the regression analysis is presented below:

$$Y_{it} = \beta_1 X1_{it} + \beta_1 X2_{it} + \beta_1 X3_{it} + \alpha_i + u_{it} \quad (3)$$

where

Y = matching percentage

X1 = performance

X2 = guidance

X3 = maturity

i = entity

t = time

β1 = coefficient for independent variable

α_i = unknown intercept for each subject entity

u_{it} = error

As Table 2: indicates, Maturity is 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 it can determined that maturity has a significant influence on the number of risks being reported by our test entities.

Performance Analysis

Another variable that was hypothesized to affect the number of risks reported by each entity is the profitability of an entity. It is hypothesized that when a company is profitable it is more inclined to disclose bad news like an increase in information security risk.

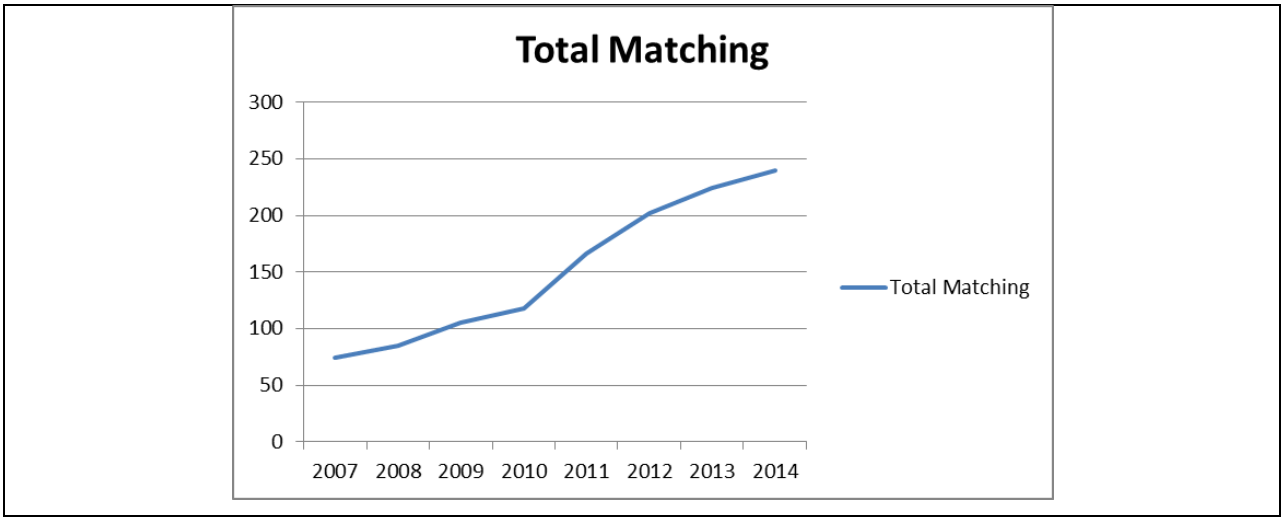
The Performance variable tells an entirely different story from the Maturity variable. In fact, the results from the "t" and "P>|t|" indicators indicate that the performance variable has no effect on the dependent variable. Therefore, for the Performance variable, the null hypothesis must be accepted. Performance does not affect risk reporting. This result is not unprecedented; in 2006 a 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 also concluded that there was no correlation between profitability and risk disclosure (Linsley, Shrives & Crumpton, 2006).

Guidance Analysis

As mentioned previously in this paper, 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 will be apparent in the 2011 reporting. Therefore, this effect will be seen from 2011 until the last year of this study, 2014.

Referring to Figure 2 Total Matching with Guidance, there is a sharp increase in reported information security risk in the 2011 10-K reports. The increase is 41% over what is reported in 2010. This increase is the largest single year increase seen throughout this study. The positive variance is nearly 100% higher than the next highest increase occurring in 2009.

FIGURE 2
TOTAL MATCHING WITH GUIDANCE



At face value it 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 being studied. Therefore, we can refer to the regression analysis numbers to confirm the significance of the Guidance variable. Regression analysis confirms the significance of guidance with a P-Value well below .05 and a t-Value of 3.06. The issuance of the guidance document therefore resulted in a 9.11% increase in the number of information security risks being reported.

Realization Analysis

The intent of this study was to collect data about information security events from each of the subject entity 8-K reports. As indicated previously, the 8-K report is used to inform investors regarding material events that occurred between postings of the quarterly 10-k reports. However, after review of the 8-K reports for the sample population, no information security risk incidents were reported. However, there were several subject entities that did have information security incidents as reported by the media (Perlroth, 2012). The previously referenced article reported that six banks had experienced sustained denial of service attacks during the week of September 24, 2012. These banks were part of this studies sample population. The banks were 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 3: Selected Entity 2011, 2012 DOS reported.

TABLE 3
SELECTED ENTITY 2011, 2012 DOS

Name	Ticker		DOS 2011	DOS 2012
JPMorgan Chase Bank, National Association	JPM		x	x
Bank of America, National Association	BAC			x
Citibank, National Association	C		x	x
PNC Bank, National Association	PNC			x
Wells Fargo Bank, National Association	WFC			x
U.S. Bank National Association	USB			x

As Table 3: Selected Entity 2011, 2012 DOS, reported indicates, prior to the publicized DOS attacks, only 2 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 indeed be occurring comes in the wake of the Target data breach of 2013. In 2013 Target announced a data breach that exposed millions of customer's financial data. The vector of the breach was malware on Target's point of sale systems (Constantin, 2014). If Realization is occurring an increase in the reporting of malware risk in 2013 would be expected. Table 4: indicates the number of entities that reported malware risk from 2011 – 2014.

TABLE 4
MALWARE REPORTED AFTER TARGET BREACH

	2011	2012	2013	2014
Malware	8	11	16	18

The results indicate there is a %45 increase in the reporting of malware after announcement of the Target security breach. This is 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 do a thorough search of all media to do a successful scientific study. Because a search of media is beyond the scope of this study, validation of the Realization variable has been abandoned.

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 business domains. The number of reported risks steadily increased throughout the study period - an encouraging sign. However, it is up to the bank regulating authorities to determine whether including 66% of risks makes the report accurate.

Two factors have been found to have an effect on the reporting accuracy of information-security risk. The first factor is maturity. As entities gained experience in reporting risks, the accuracy of their reporting increased. The other factor is guidance. When the SEC published a guidance document telling companies what to report and how to report it, accuracy increased. This increase in reporting accuracy due to guidance is an important result and demonstrative of how simple instructions can increase the accuracy of risk reporting. While this study focused on information security risk, guidance could be used for other risks as well.

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. So it is not surprising that information- security risk reporting accuracy 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, the realization effect 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.

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 publically traded corporations regulated by the SEC to provide a generalizable result.

Publically traded corporations should be reporting incidents such as security breaches on their 8-K reports, but they are not. This lack prevented this study from scientifically determining if realization of a threat increased the likelihood of reporting that threat's corresponding risk. Another study could be undertaken that circumvents this lack of 8-K reporting, one that could use other means, such as the media, to determine which threats were becoming known as a result of a breach.

Because of the general nature of the risk statements made on the 10-K report, it was necessary for this study to group risks into broad categories. It is likely that risks being reported on the 10-K report will become more specific because the process matures and entities continue to become aware 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

Acquisti, A., Friedman, A., & Telang, R. 2006. Is There a Cost to Privacy Breaches? An Event Study, in Proceedings of the 27th International Conference on Information Systems, Milwaukee, WI, pp. 1563-1580.

Aguilar, L. (Commissioner) (2014, June 10). Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus. *Cyber Risks and the Boardroom Conference* . Lecture conducted from New York Stock Exchange, New York, NY.

Baltagi, B. (2008). *Econometric analysis of panel data* (Vol. 1). John Wiley & Sons.

Bhide, A. (1993). The hidden costs of stock market liquidity. *Journal of Financial Economics*, 34(1), 31-51.

Campbell, J. L., Chen, H., Dhaliwal, D. S., Lu, H. M., & Steele, L. B. (2011). The information content of mandatory risk factor disclosures in corporate filings. *Review of Accounting Studies*, 1-60.

Constantin, L. (2014, January 14). Target point-of-sale terminals were infected with malware. Retrieved March 23, 2015, from http://www.pcworld.com/article/2087240/target-pointofsale-terminals-were-infected-with-malware.html

Creswell, J. W., & Clark, V. L. P. (2007). *Designing and conducting mixed methods research* (p. 275). Thousand Oaks, CA: Sage publications.

Eisenhardt, K. (1989). Agency Theory: An Assessment and Review. *The Academy of Management Review, 14*(1), 57-74.

Ferraro, M., (2013), 'Groundbreaking' or Broken? An Analysis of SEC Cyber-Security Disclosure Guidance, Its Effectiveness, and Implications (May 5, 2013). *Albany Law Review*, Vol. *77*, 2014.

Gibbs, J. P. (1975). *Crime, punishment, and deterrence* (p. 58). New York: Elsevier.

Greene, *William H. Econometric analysis* / 6th ed., Upper Saddle River, N.J. : Prentice Hall, 2008.

Helbok, Guenther & Wagner, Christian (2006), Determinants of Operational Risk Reporting in the Banking Industry (July 11, 2006). Available at SSRN: http://ssrn.com/abstract=425720 or http://dx.doi.org/10.2139/ssrn.425720

IAS Plus. (2014, March 21). CAQ publishes cybersecurity alert. Retrieved May 9, 2014, from http://www.iasplus.com/en-us/news/2014/03/caq-alert-cybersecurity

Jorion, P. (1996). Risk2: Measuring the risk in value at risk. Financial Analysts Journal, 47-56.

Keller, E. (1988). Introductory comment: a historical introduction to the Securities Act of 1933 and the Securities Exchange Act of 1934. *Ohio State Law Journal*, *49*, 329-352.

Kothari, S., S. Shu, & P. Wysocki. 2009. Do managers withhold bad news? *Journal of Accounting Research* 47: 241-276

Linsley, P. M., Shrives, P. J., & Crumpton, M. (2006). Risk disclosure: An exploratory study of UK and Canadian banks. *Journal of Banking Regulation,7*(3), 268-282.

Macey, J. R., & Miller, G. P. (1991). Origin of the Blue Sky laws. *Texas Law Review*, *70*, 347.

McGrath, M. (2014, February 26). Target Profit Falls 46% On Credit Card Breach And The Hits Could Keep On Coming. Retrieved April 28, 2015, from http://www.forbes.com/sites/maggiemcgrath/2014/02/26/target-profit-falls-46-on-credit-card-breach-and-says-the-hits-could-keep-on-coming/

Mirakur, Y. Risk Disclosure in SEC Corporate Filings. *Wharton Research Scholars Journal*. Retrieved May 7, 2014, from http://repository.upenn.edu/wharton_research_scholars/85/

Perlroth, N. (2012, September 30). Attacks on 6 Banks Frustrate Customers. Retrieved April 10, 2015, from http://www.nytimes.com/2012/10/01/business/cyberattacks-on-6-american-banks-frustrate-customers.html?_r=1

Saad, L. (2013, May 1). U.S. Stock Ownership Stays at Record Low. U.S. Stock Ownership Stays at Record Low. Retrieved April 18, 2014, from http://www.gallup.com/poll/162353/stock-ownership-stays-record-low.aspx

Securities and Exchange Commission. (2005). Final rule: Securities offering reform (SEC Release No. 33-8591). Washington, DC: Government Printing Office. Retrieved from http://www.sec.gov/rules/final/33-8591.pdf

Skinner, D. J. (1994). Why firms voluntarily disclose bad news. *Journal of accounting research*, *32*, 38-38.

Stoneburner, G., Goguen, A., & Feringa, A. (2002). Risk management guide for information technology systems. *Nist special publication*, 800-30.

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

Williams, C. (1999). The Securities and Exchange Commission and Corporate Social Transparency. *Harvard Law Review, 112*(6), 1197-1311.

Yelle, L. E. (1979). The learning curve: Historical review and comprehensive survey. *Decision Sciences*, *10*(2), 302-328.

Yin, R. K. (1994). *Case study research: design and methods* (2nd ed.). Thousand Oaks: Sage Publications.