Reading the Disclosures with New Eyes: Bridging the Gap between Information Security Disclosures and Incidents [†]

Ta-Wei "David" Wang
Krannert Graduate School of Management
Purdue University
West Lafayette, IN 47907-2056
wang131@purdue.edu

Jackie Rees
Krannert Graduate School of Management
Center for Education and Research in Information Assurance and Security (CERIAS)
Purdue University
West Lafayette, IN 47907-2056
jrees@purdue.edu

Oct. 31, 2007

Abstract

This paper investigates whether information security related disclosures in financial reports can mitigate the impacts of information security incidents. First, by drawing upon the theories in accounting literature, we regress stock price reactions to a number of information security related incidents from 1997 to 2006 on the number of disclosures along with control variables. Two different types of disclosures are considered: disclosures of internal control and procedures and disclosures of information security risk factors. Our results do not provide enough evidence to clearly link the disclosures of internal control and procedures with stock price reactions to information security incidents. However, our findings demonstrate that new information security risk factor disclosures can mitigate the effect of information security incidents in terms of cumulative abnormal return (CAR). Furthermore, whether the disclosures match the incidents does not affect stock price reactions. Instead, our results show that for the matched companies, other business risk factors can adversely increase CAR. Second, a clustering analysis is performed on information security risk disclosures and media announcements of the incidents using text mining techniques. The clustering results demonstrate that the titles and contents of the disclosures point out possible impacts and subjects that might be affected. For media announcements, site attacks and virus attacks are the two most popular incidents in our sample from the clustering analysis. This paper not only contributes to the literature in information security and accounting but also sheds light on how managers can evaluate their information security policies and convey information security practices more effectively to the investors. By properly reflecting information security risk factors caused directly by information security incidents and indirectly by other companies, investors might discount the impacts of such events through expectation formulation.

Keywords: information security, Sarbanes-Oxley Act (SOX), risk disclosure, event study

---

[†] The authors are grateful to CERIAS for funding part of the research.

1. Introduction

Organizations rely heavily on information technology (IT) to enable daily operations. Because of this dependency on IT, there may be a tremendous impact when there is an information security related incident. For example, a series of Denial of Service (DoS) attacks in 2000 resulted in online retailers and portals such as Amazon.com and Yahoo! losing service for hours (Sandoval and Wolverton 2000). According to the CSI/FBI computer crime and security report in 2006 (CSI/FBI 2007), the total dollar amount of financial losses resulting from security breaches is approximately $200,000 US dollars per respondent. The losses of different types of attacks ranged from $90,000 to $15,000,000, accompanied by the fast growing number of reported security incidents (CERT 2007). This evidence highlights the organizational concerns generated by information security incidents and the accompanied shareholders' concerns.

Given such concerns, evaluation of the impacts of information security incidents is not only used for managerial decisions but also conveyed to investors and the public. We observe two pieces of information disclosed by companies in annual or quarterly reports regarding information security. One is the internal control report, which is mandated by Sarbanes-Oxley Act (SOX)[1] Section 404, describing the weaknesses of internal controls and financial systems. A weak financial system infrastructure can influence the quality of financial statements which might lead to bad decisions by debtors and investors because of an inaccurate estimation of business value. The other piece of information is the disclosure of risk factors. Some companies voluntarily disclose risk factors that might adversely affect their business, such as fierce competition or a change in consumer preferences. Information security related risk factors, such as the impact of viruses or DoS attacks, might also be voluntarily disclosed in financial reports.

[1] H. Res. 107-414, 116 STAT. 745 Cong. Rec. 5395 (2002) (enacted). Retrieved on Apr. 9 2007, from http://news.findlaw.com/hdocs/docs/gwbush/sarbanesoxley072302.pdf

Discretionary disclosures have long been studied in the accounting literature under the assumption that managers possess more information than outsiders (Healy and Palepu 2001; Verrecchia 2001). By disclosing some credible information that implies a higher value of the firm, the company's value can be revised (e.g. Grossman 1981; Lev and Penman 1990). Voluntary disclosures thus can reduce cost of capital or cost of debt and increase stock liquidity (e.g. Amir and Lev 1996; Botosan 1997; Lang and Lundholm 1996). Furthermore, firms can achieve the same level of information security at a lower cost by sharing security-related information (Gordon et al. 2003). One recent study by Sohail (2006) also points out that information security related discretionary disclosures are positively related to stock price.

Building on the theories in accounting literature, we expect that an organization should be willing to disclose information security related risk factors that might interrupt business operations or alter financing and investment decisions in financial reports. These disclosures can inform the readers about possible risk factors the organization is facing. By incorporating these factors, user form expectations of the company's performance while making investing or financing decisions. Therefore, it is expected that the extent of the surprise is smaller for disclosing companies if those information security concerns are articulated in advance. However, given all these current disclosures, no matter if mandatorily or voluntarily disclosed, we might or might not observe a huge drop in stock price after information security incidents. For example, Yahoo!, eBay, and Buy.com were all hit by DoS attacks in February 2000. After the attack, the stock prices for Yahoo! and eBay rose. But meanwhile, the stock price for Buy.com fell about 17% even it was the day Buy.com went public and even with the disclosure[2] about the impacts of

[2] In the news article, Tran and Rundle (2000) wrote that "Buy.com's listing of risk factors included a caution that 'System failures could prevent access to our online store and harm our business…[and] cause customer dissatisfaction or damage our reputation'".

system failure (Tran and Rundle 2000). Also, from a random pilot sample of thirty companies, we observe that companies rarely point out the impacts of these information security factors on their business. Consequently, this paper tries to bridge the gap between information security disclosures and incidents and to address the following research questions: Do information security disclosures in financial reports mitigate stock price reactions when a company faces information security incidents?[3] What are the elements within these disclosures that have significant impacts on stock prices or investor's expectation formulation? What are the kinds of disclosure content that characterize these disclosures?

Several studies have investigated the impact of security incidents on business value in terms of stock price reactions. Some of such studies find significant negative impact (Ettredge and Richardson 2003; Garg et al. 2003) while others do not find such evidence (Campbell et al. 2003; Cavusoglu et al. 2004; Hovav and D'Arcy 2003; Kannan et al. 2007) given different data sets and methodology. Furthermore, as suggested by anecdotal evidence, companies that suffered from security breaches do not always show material effects on their financial reports in terms of operational performance (Kannan et al. 2007). Since not all sources of information security risk can be enumerated and identified, and the likelihood of security incidents is difficult to measure, we need to formulate possible strategies to appropriately manage this risk given it is impossible to perfectly eliminate security concerns. In order to manage information security risk, we need to understand the impacts and how to mitigate the risks (Borge 2001; Frame 2003; Focardi and Jonas 1998). Consequently, as an initial step of our research, we attempt to analyze the impacts

[3] We focus on the disclosures of possible risk factors in financial reports instead of the disclosures of security breaches or sharing vulnerabilities. The latter has been addressed by, for example, Gal-Or and Ghose (2005), Gordon et al. (2005).

of voluntary disclosures of information security risk factors on stock prices.[4] Furthermore, since how the risk factors are disclosed in financial reports and the readability of financial reports can affect investors' expectations (Katz 2001; Li 2006), we also investigate the contents of risk factor disclosures using text mining techniques to address the second and the third research questions. By understanding how the risk factors are conveyed to the public, we demonstrate how investors' expectations are formed and provide additional explanations of the impacts of information security from a different perspective.

Our major findings are summarized as follows. First, we do not uncover a clear relationship between the disclosures of internal controls and the stock price reactions because of the relatively standardized contents of the disclosures of internal control and procedures. However, the disclosures of information security risk factors can mitigate the impacts of information security incidents for breached companies. Our results also demonstrate that repeated disclosures do not have the same impacts as first time disclosures. The rationale behind the observation is expectation formulation (Ajinkya et al. 1984; King et al. 1990). Investors can form expectations of future impacts of information security incidents through these disclosures thereby mitigating the actual impact. Furthermore, similar to Campbell et al. (2003), we show that confidentiality and integrity types of information security incidents have more impacts on CAR than availability type incidents since the direct and indirect impacts of such incidents are less than the former ones. Second, because investors tend to focus more on the overall impacts of incidents, whether the incidents match the risk factors disclosed does not lower the surprises of information security

[4] Sohail's (2006) focus is to assess the market value of all the voluntary disclosures of information security activities, i.e. whether the market values discretionary disclosures of information security activities or whether discretionary disclosures of information security activities are positively correlated with stock price. Our paper also investigates the relationship between stock price reactions and financial reports disclosures in the context of information security incidents, but the primary goal is to understand whether disclosures in financial reports can mitigate the corresponding negative impacts in terms of stock price reactions.

incidents. Moreover, the role played by company size varies for the experimental group and the control group. For the experimental group, company size helps the company against the shock. However, company size might cause a non-breached company to become a target in the future. Last, the clustering results from text mining demonstrate that both the titles and contents convey the impacts of information security incidents and the possible affected subjects of the company to the public. The clustering analysis also shows that breached companies gradually increase the number of disclosures than non-breached firms does. But for media announcements, the clustering results show that site attacks and virus attacks appear to be the two most frequently reported incidents in our sample.

The contributions of this paper are two-fold. First, our paper contributes to the literature of information security and practitioners. For researchers, our results further address the issue on the value of information security related activities and disclosures. We provide evidence on how investors might perceive information security risks disclosed in annual or quarterly reports. The explanations can be considered when conceptualizing risk management strategies. For practitioners, the results shed light on how they can convey security practices to their customers more effectively. Disclosures of information security risk factors can be an important way to mitigate the impact of information security incidents in terms of business value. Managers can disclose possible information about security risk factors to investors as a means to manage expectations.[5] As shown by the text mining results, the titles and contents have already reflected possible impacts. The disclosures will be used for investors to discount the impacts of information security incidents because they have already incorporated such risks as part of the business operations. Also, managers can prevent firms' value from decreasing by disclosing

[5] In this paper we do not attempt address the research question about the optimal level of disclosures, which has been extensively studied in accounting literature.

such information. Nevertheless, though it is not our main result, information transfer still seems to exist in our sample. Managers might need to consider the impacts from other companies when formulating information security strategies or when evaluating the impacts of information security incidents. Companies in the same industry can also work together to lower the impacts of information security incidents. More importantly, since the company needs to generate the information for disclosures and investors value such disclosures, the executives can evaluate the effectiveness of information security governance at the same time. The effectiveness can also be conveyed to the public as another means of expectation formulation of the investors. Second, this paper adds to the discretionary disclosure literature. We focus on a specific category of voluntary disclosures in annual or quarterly reports and examine the related impacts of such disclosure. The literature shows that when disclosures can increase a firm's value, managers are willing to release such information. Our results demonstrate that disclosures of risk factors can help prevent a firm's value from decreasing for the experimental group. Thus, we add to the literature that when disclosures have non-negative impacts on a firm's value, managers should also be willing to disclose such information. Furthermore, our results show that the companies in the control group disclose less than the experimental counterpart for this kind of information. The fully revealing outcome or the partially revealing outcome (Milgrom 1981; Verrechia 1983; Dye 1985)[6] in voluntary disclose literature might not be applied since we do not suspect that the

[6] The idea of fully revealing is proposed by, for example, Milgrom (1981). The rationale behind this fully revealing result is "signaling". In these studies about voluntary disclosure, if managers have information that imply a higher business value than the average of all the companies in the market, managers will disclose such information thereby resulting in an increase in stock prices. Meanwhile, investors consider those non-disclosing companies to have business values less than the market average. Thus, the perceived valuation of these non-disclosing companies is adjusted downward. This adjustment then urges the non-disclosing companies with "good news" to disclose the information in order to distinguish themselves from others. This process stops until all the companies reveal their relative valuation position in the market. The partially revealing outcome is argued by, for instance, Verrechia (1983) and Dye (1985). Verrechia (1983) and Dye (1985) show that when there exists disclosure costs or investors are not able to distinguish whether no disclosure results from either (1) managers have no information or (2) managers are not willing to disclose, some companies voluntarily disclose information but some do not.

disclosure costs vary across companies with similar market capitalization in the same industry. The uncertainty for investors is also not possible for disclosures of information security risk factors because many these factors are similar for companies in the same industry. It seems that the impact of this "negative" type information needs to be further understood in addition to other voluntary disclosures. Moreover, the exploratory text mining results can be seen as a first step in understanding the real information released in financial reports. Based on the preliminary understanding of these disclosures, the impact of textual disclosures can be further elaborated.

2. Literature Review

There are two major streams of literature related to our study. One is the research in information security. The other is the literature on disclosures in accounting.

2.1 Literature review in information security

A majority of information security literature focuses on technical issues (Sohail 2006). For example, it is expected that the frequency of security breaches can be reduced with a better access control (Sandhu 1996). On the other hand, analytical and empirical studies in information security from an economic perspective are relatively limited (Sohail 2006). For instance, Gordon et al. (2006) demonstrate that, after SOX was enacted, managers have put more attention on corporate information security activities. Several studies have been done to address information security investments analytically. For example, Gordon and Loeb (2002) propose an economic model to determine the optimal investment in information security. Also, Gordon et al. (2003) examine the organizational investments in information security in an information sharing environment.

Studies have also pointed out that information security breaches can result in material impacts of business operation, including physical and intangible impacts such as negative

company image and loss of reputation (Glover et al. 2001; Warren and Hutchinson 2000). Several empirical studies have been done to investigate the impact of information security events on business value. Based on different methodology and different data sets, some of the results show that there exist significant negative impacts (Ettredge and Richardson 2003; Garg et al. 2003), while others do not find such impact (Campbell et al. 2003; Cavusoglu et al. 2004; Hovav and D'Arcy 2003; Kannan et al. 2007). For example, Ettredge and Richardson (2003) investigate the impacts of the denial of service attacks which happened in February 2000 and attempt to determine which company might suffer or benefit from similar incident in the future. Their results demonstrate the existence of information transfer and show that the larger the company, the larger the abnormal return. Campbell et al. (2003) examine whether information security incidents affect market values and find that there exists a negative impact on market value but that impact is not statistically significant. However, confidentiality type incidents indeed result in a significant and negative impact on market value. Kannan et al. (2007) also analyze short-term and long-term impacts of security announcements on market value and do not uncover a relationship between announcements and business value. The relationship between information security and information disclosures has also been examined in the literature. For example, Sohail (2006) assesses the market value of information security disclosures and demonstrates that security disclosures are positively and significantly related to stock price.

2.2 Literature review on disclosures in accounting

There is a rich body of literature examining voluntary disclosures in accounting. Analytical studies in voluntary disclosures generally assume that there is no disclosure cost and the disclosures are credible (e.g. Grossman 1981). In this case, full disclosure exists because investors believe that non-disclosing companies have the worst possible information (e.g.

Grossman 1981). But if disclosure costs exist, only when the benefits exceed the costs will companies disclose (e.g. Verrecchia 1983). The disclosure decision also depends on whether such disclosure will provide information to competitors and depends on mandatory disclosures (e.g. Verrecchia 1983; Darrough 1993; Eihorn 2005).

Furthermore, several empirical studies focus on the quality and credibility of the disclosures (e.g. Lang and Lundholm 1993; Penno 1997; Stocken 2000), the usefulness of disclosures (e.g. Francis et al. 2002; Landsman and Maydew 2002), and other aspects of voluntary disclosures such as costs, analysts following, and signaling rationale (e.g. Elliott and Jacobson 1994; Lang and Lundholm 1996; Lev and Penman 1990). For example, Lang and Lundholm (1993) show that a company's performance can be linked to the quality of disclosures. Skinner (1994) demonstrates why firms are willing to voluntarily disclose bad news. Moreover, Ajinkya and Gift (1984) and King et al. (1990) both discuss that voluntary disclosures in financial reports can be used to adjust analysts' and investors' expectations. Narrative disclosures in Management's Discussion and Analysis (MD&A) can also influence financial analysts' forecasts (Barron et al. 1999) and the forecast precision is related to the stock price reactions to management earnings forecasts (Baginski et al. 1993; Pownall et al. 1993).

3. Research Framework and Hypotheses Development

Based on the discussion in the previous section, we formulate our research framework as Figure 1. Each company faces numerous potential information security risks that are defined based on concepts proposed by the National Institute of Standards and Technology—Computer Security Resource Center (NIST-CSRC) (Bowen et al. 2006). Those information security risks can be categorized as one of three types: (1) confidentiality, such as theft of source code or customer data, (2) integrity, such as a virus attack which deletes or alters files, and (3)

availability, such as denial-of-service attacks (Bowen et al. 2006; Gordon et al. 2006). Given the threats posed by these risks, each company discloses two elements in the annual or quarterly financial reports. The first element is "management assessment of internal controls" (hereafter referred to as the disclosures of internal control and procedures) which is mandated by SOX section 404 (refer to Appendix A for definitions). An example of the disclosures of internal control and procedures is provided in Appendix B. The second element is risk factors or the possible uncertainties regarding forward-looking statements. Managers identify possible risk factors that may adversely affect a company's future performance in terms of operation, customer relationship, etc. Some companies also include information security related risk factors when disclosing risk factors. Examples of such disclosures are provided in Appendix C.

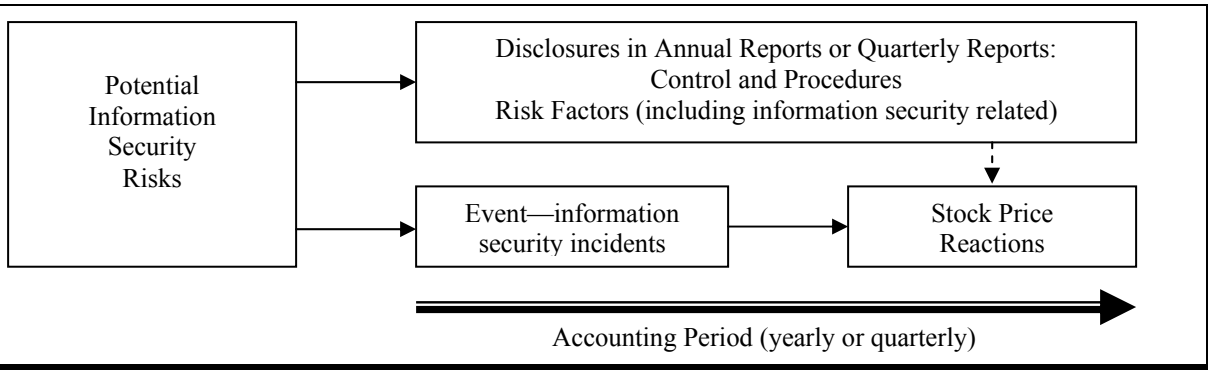

Figure 1. Research Framework

As shown in Figure 1, companies may encounter information security incidents, such as a virus attack or DoS attacks, in a given time period (or accounting period). Based on the theory of market efficiency (Fama 1970), people can expect some level of stock price reactions after the incident is disclosed. Meanwhile, both numerical and narrative signals from financial reports affect how users formulate expectations of a company's future performance. Further, if voluntary disclosure can increase the value of the firm, managers are willing to disclosure such information (e.g. Milgrom 1981; Grossman 1981; Verrecchia 1983; Dye 1985; Lev and Penman

1990; Verrecchia 2001). Voluntary disclosures are also positively and significantly related to stock price (Sohail 2006). Since information security incidents may have negative impacts on a firm's value, it is expected that information security related disclosures can prevent a firm's value from decreasing. Consequently, we argue that the disclosures of control and procedures as well as risk factors (in this case, information security related risk factors) should be able to help financial report users form expectations of possible future incidents which may adversely affect the company's performance. These expectations can in turn affect the magnitude of the stock price reactions due to information security incidents because investors have already discounted the effects of such incidents (shown as the dotted line in Figure 1). Based on the discussion above, we have our research proposition.

Proposition: Information security related disclosures in annual or quarterly financial reports mitigate the impact of information security incidents on business value in terms of stock price reactions.

As mentioned previously, there are two possible information security related disclosures. The first one is the disclosures of internal control and procedures. Though information security is not the primary focus of these disclosures, they somehow reveal information about the controls needed to ensure the quality of financial reports. Therefore, in order to test our proposition empirically, we formulate our first hypothesis.

Hypothesis 1: For breached firms, as the number of internal control related items disclosed in the section of "Control and Procedures" increases, the impact of information security incidents on stock prices decreases.

The second possible information security related disclosure is the disclosure of information security risk factors in the section of all the risk factors or uncertainties regarding forward-

looking statements. In these sections, companies specify important factors that may adversely affect future performance. Information security risk factors are sometimes also covered. Investors may then have a clear picture of the impact of information security incidents on business performance. Consequently, we state our second hypothesis.

Hypothesis 2: For breached firms, as the number of disclosures of information security related risk factors increases, the impact of information security incidents on stock prices decreases.

As discussed, the rationale behind hypothesis 2 is that the disclosures of information security related risk factors can help financial report users form expectations of possible future incidents. The expectations can affect the magnitude of the corresponding stock price reactions of such incidents. However, there are three more issues with regard to this argument which are not tested directly in hypothesis 2. First, from the argument, the effect on stock price reactions results from the formulated expectation. That is, the disclosed risk factor help formulate users' expectations first. Then the company actually experiences that specific risk factor with a stock price reaction. For example, a company mentions the effect of virus attacks in the annual report and the company actually suffers from virus attacks. After the media announces the attacks, the stock price reacts to such incident. However, in hypothesis 2, we do not explicitly consider when the information security incident a company faces matches the disclosed information security risk factors in financial report, the impact on stock price reactions decreases or not. Therefore, hypothesis 3 is built to take this issue into account.

Hypothesis 3: For breached firms, if the information security risk factors disclosed by a company in financial reports match the incident the company suffers, as the number of disclosures of information security related risk factors increases, the impact of information security incidents on stock prices decreases.

The second issue related to the argument is also expectation formulation. Disclosures in annual reports may not provide useful additional information since the same content could have already been disclosed in previous years' reports. For example, a company discloses possible impacts of virus attacks in annual report every year starting from 2002. When this risk factor is first disclosed in 2002, report users might form expectation of the impact of virus attacks. However, when users see the same disclosure in the annual report again and again from 2003 until now, there is no new information and no new expectations. That is, risk factors that have already been disclosed in previous years' annual reports might not play the same role as those that are disclosed for the first time because expectations have already been formed. Thus, we further distinguish disclosures from acknowledgments, which are the information that has already been disclosed. We state our fourth hypothesis as follows.

Hypothesis 4: If information security related risk factors stated in current year's financial report have already been disclosed in previous years' financial report(s), as the percentage of repeated disclosed information security related risk factors in previous years' financial reports increases, the impact of information security incidents on stock prices decreases.

A conceptual model of the development of the hypotheses is provided in Figure 2.

The third issue relates to how expectations are formed. We need to further understand the contents of the disclosures in order to draw relationships among disclosures, expectation

formulation, information security incidents, and stock price reactions. If the contents of the disclosures demonstrate the impacts of information security incidents and/or the affected units or subjects, we are more confident with the argument and the theory we draw upon. Further, the contents might also help us better explain the phenomenon under investigation. This issue is taken into account by applying text mining techniques which are elaborated in section 4.2.3.

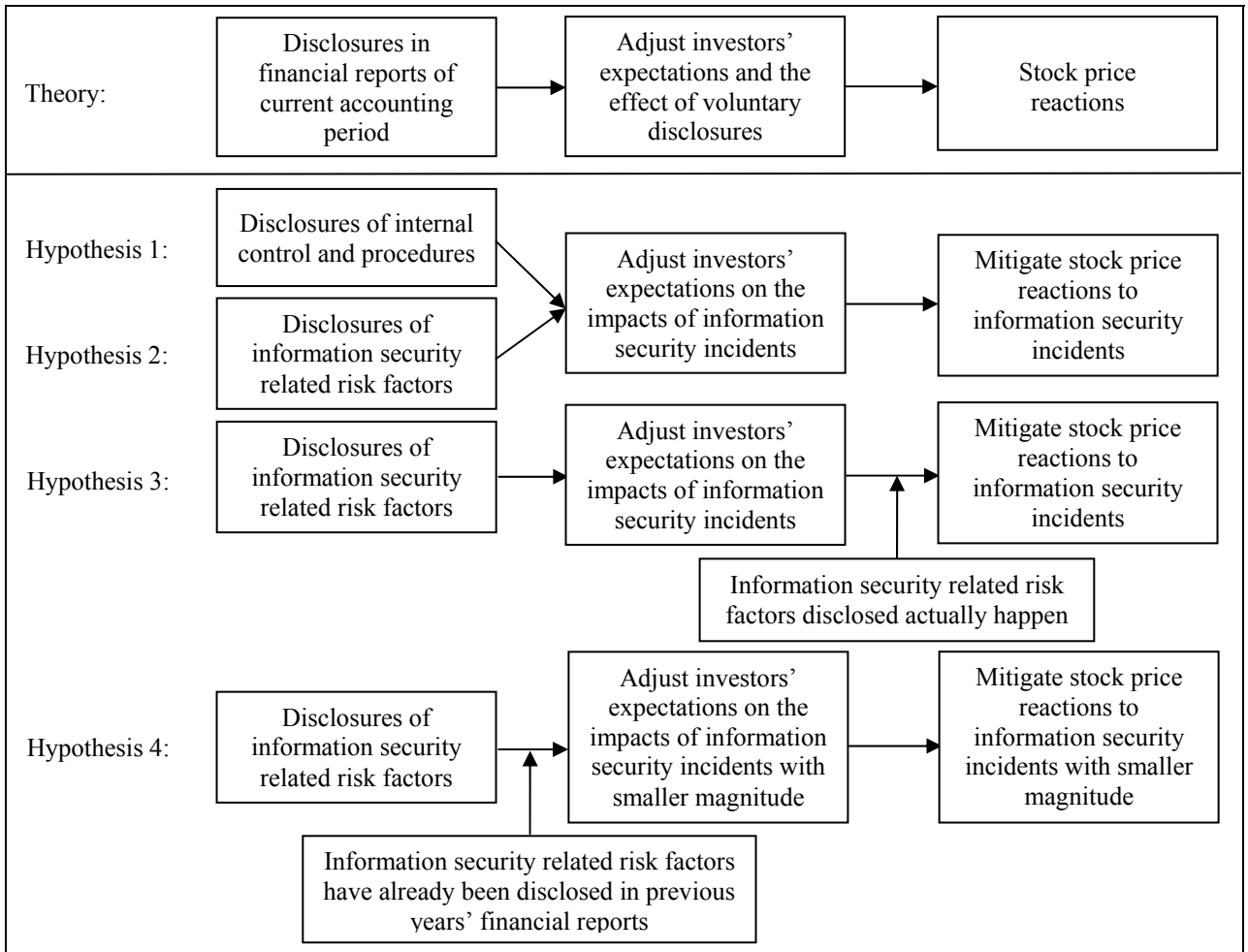

Figure 2. Conceptual Model of the Development of the Hypotheses

4. Empirical Analysis

Based on our proposition and hypotheses, we need to first identify information security incidents. Second, based on those events, we filter out necessary control and procedures as well as risk disclosure contents in financial reports and the associated stock prices. Last, we

investigate the relationship between the reactions of stock price and the corresponding control and risk disclosures in financial reports.

4.1 Sample Selection

To identify security incidents, we search for news with the following keywords in the time period from 1997 to 2006 in the *Wall Street Journal*, *USA Today*, the *Washington Post*, and the *New York Times* via the Factiva database as well as in *CNet* and *ZDNet*. The keywords are: (1) security breach, (2) hacker, (3) cyber attack, (4) virus or worm, (5) computer break-in, (6) computer attack, (7) computer security, (8) network intrusion, (9) data theft, (10) identity theft, (11) phishing, and (12) cyber fraud, which are similar to the keywords used in prior studies (e.g. Campbell et al. 2003; Garg et al. 2003; Kannan et al. 2007). While searching for the news, we check whether the companies release such information on their websites before the media does as a robustness check for the timing of the incidents and the reaction of the stock prices. For our sample, we do not encounter any self-disclosed information directly from the companies. Samples with the following properties are then filtered out. First, the news must identify or enable us to identify a specific event date of the corresponding security incident. Second, only publicly traded firms are included. We delete the news related to government agencies and privately held firms from our sample. Last, annual reports (10-K reports) or quarterly reports (10-Q reports) of the sample firms are available for the corresponding period from EDGAR Online[7]. For the corresponding period, we consider several possibilities. First, the financial reports released one period before the incidents. For instance, if the event occurs on February 8 year 2000, we can use the annual report for 1999. However, for different companies, the reporting date can be different. Companies may release the report in March or April in 2000, i.e.

[7] http://www.sec.gov/edgar/searchedgar/webusers.htm

after the incident, which is not consistent with our selection criteria. Further, for different companies, we might need to use reports in different years even the event occurs on the same date thereby causing a comparison problem. Second, we can use the quarterly reports released before the security events. However, the comparison problem mentioned above might still exist. Furthermore, many companies only disclose risk factors in annual reports since those factors generally do not change from quarter to quarter. In this case, we are not able to collect the required data. Consequently, in our paper, the corresponding period mostly refers to the fiscal year those incidents occur unless under the condition that annual reports are unavailable, such as the last year of listing. The resulting sample consists of 108 firm-event observations (61 observations are before year 2002 and 47 are after 2002, including 2002, which is the year that SOX came into effect). A list of the firms in our sample is provided in Appendix D.[8]

For each breached firm, we match it to one of its competitors that does not suffer from information security incidents on the same date as the controlled company. We gather this information from Yahoo! Finance and the Hoover's Database. The selection criteria are as follows. First, the competitor must not have suffered from information security incidents on the same date. Second, the annual reports are also available for the competitor. Third, if several competitors can be selected, we choose the one with similar market capitalization. A list of our control companies is also provided in Appendix D.

We collect the following data from our news sample and companies' financial reports for both the experimental and control group: (1) Company identification information: company name, first two-digit of industry identification code (SIC code), and CUSIP number for each

[8] Two issues regarding our sample are worth noting here. First, three companies were attacked in consecutive three days in February 2000. However, these nine observations (three companies in three days) do not bias our result because the effects on stock price do not show a consistent trend (neither positive nor negative) across companies and across three days. Second, as expected, Microsoft is the biggest target in our sample. However, since Microsoft does not disclose any information security related risk factors for most of the years, it does not affect our main result.

company's stock. (2) Security incident information: the title of the news, event date, source of the news and the content. (3) Financial reports information: which report (10-K or 10-Q) and which year of the report we use, disclosures in the "Control and Procedures" section, and information security related and all risk disclosures. As mentioned above, security related disclosures are defined as either confidentiality, integrity, or availability (Bowen et al. 2006; Gordon et al. 2006). The descriptive statistics of our sample is provided in Table 1 and Table 2. Interestingly, Table 1 demonstrates that there seems to be a shift from integrity and availability type incidents to confidentiality type.[9] The shift might result from the growing value of data for criminals (i.e. identity theft).

Table 1. Sample Distribution			
Type of Incidents	Confidentiality	Integrity	Availability
Number of Firm-Year Observations	38	32	44
Number of Observations in Year			
1997	0	0	2
1998	0	1	1
1999	1	16	5
2000	8	3	16
2001	4	2	4
2002	3	0	4
2003	3	5	9
2004	3	4	3
2005	8	0	0
2006	8	1	0

Table 2 shows that, on average, there is a greater number of security related disclosure and total number of risk factors disclosed per firm-event observation after year 2002, which is consistent with Gordon et al. (2006). The number of information security related risk factors and the total number of risk factors are calculated as follows. We count how many factors (both the total number of risk factors and information security related risk factors) mentioned by the

[9] Six observations are grouped into both the integrity type and the availability type. For example, the "I love you" worm not only destroys files (integrity type) but also slows down mail server systems (availability type). Furthermore, two raters performed the coding task. We do not consider these six observation for reliability since these six observations were dropped from the analysis for the types of incidents later. Given the high inter-rater reliability (Cohen's $\kappa = 92.83\%$), we adopt the author's coding results for later analysis.

company in annual reports or quarterly reports under the section of risk factors or the section of forward-looking statements.[10] For instance, as shown in Appendix C, one risk factor disclosed by Amazon in year 2000[11] named "We face intense competition". The other is "System interruption and the lack of integration and redundancy in our systems may affect our sales". Thus, after looking into the content of the disclosures, we count one for information security related risk factors and two for total risk factors in this case. We choose this method because companies generally group several elements which might result in similar consequences in one risk factor. Therefore, we posit that general investors take these elements as a whole or as a single factor and evaluate the impacts on that specific company.

Table 2. Descriptive Statistics of Disclosures

Control and Procedures Disclosures	Percentage of Disclosures before 2002		Percentage of Disclosures after 2002[a]		Total	
	Experimental	Control	Experimental	Control	Experimental	Control
Evaluation	0.00%	0.00%	53.19%	97.73%	23.15%	48.31%
Management	0.00%	0.00%	74.47%	36.36%	32.41%	17.98%
Change	0.00%	0.00%	48.94%	56.82%	21.30%	28.09%

Risk Factor Disclosures	Number of Security Related Disclosures				Total Number of Risk Factors Disclosed			
	Experimental		Control		Experimental		Control	
	before 2002	after 2002	before 2002	after 2002	before 2002	after 2002	before 2002	after 2002
Total	39	56	3	17	837	856	502	806
Average (stdev)	0.64 (1.304)	1.91 (1.469)	0.07 (0.327)	0.39 (0.655)	13.72 (9.830)	18.21 (11.205)	10.91 (7.725)	18.32 (9.243)
Max (min)	4 (0)	5 (0)	2 (0)	3 (0)	38 (0)	45 (0)	38 (0)	47 (5)

[a] SOX was enacted in 2002

[10] The keywords mentioned previously are solely used for identifying events not for data coding. We have also designed a more complicated coding scheme. However, since our sample includes companies from different industries, the coding scheme cannot be consistent across industries and companies especially for business risk factors. Furthermore, again since two raters' inter-rater reliability is high for both groups (Cohen's κ = 97.23% and 100% respectively), the author's coding results are used.

[11] http://www.sec.gov/Archives/edgar/data/1018724/000103221001500087/0001032210-01-500087.txt

4.2 Analysis

4.2.1 Event study

It has long been an important issue for economists as well as accounting and finance researchers to understand the impact of economic events on business value (MacKinlay 1997). According to the theory of market efficiency (Fama 1970), such events should be reflected immediately by the stock prices. Therefore, the impact of economic events on business value can be measured by the stock price reactions in a short period of time (MacKinlay 1997). An event study measures the impact on business value of a certain event using financial data (MacKinlay 1997). Consequently, event study is performed as a first step in our study to capture the impact of security incidents. Based on our firm-event observations, we are able to conduct an event study applying the market model:

$$R_{it} = \beta_0 + \beta_1 R_{mt} + \varepsilon_{it} \quad (1)$$

where R_{it} denotes company i's return at period t which equals to $(p_t - p_{t-1}) / p_t$, i.e. the percentage change in prices across two periods.[12] R_{mt} stands for the corresponding market return at period t and is estimated by the CRSP equally weighted index. The CRSP equally weighted index is the average of the returns of all trading stocks, i.e. $R_{mt} = (\Sigma R_{it}) / N_t$, where N_t is total number of trading stocks all at period t. β_0 and β_1 are the parameters and are estimated in a 255-day periods ending at 45 days before the estimation window we choose by ordinary least square (OLS) method. Equation (1) emphasizes the effects that cannot be explained by the market (i.e. ε_{it}), which is the reaction resulting from the economic event. To conduct the event study, samples with confounding events, such as earning announcements and stock splits, are first eliminated so as to avoid possible other causes to the stock price reaction. Also, we must have

[12] Dividends and stock splits are excluded because (1) they are rare events and (2) we have already considered confounding events. Thus, stock return of a certain company equals to the change in stock price or the capital gain.

stock price information in order to perform our study. The resulting sample size becomes 90 firm-event observations for the experimental group. For our control group, we further control for the spillover effect. The spillover effect or an information transfer exists when an economic event of one firm affects another firm's (or other firms') stock price(s) (Foster 1986). As shown by Ettredge and Richardson (2003), in our research context, it is highly likely that the security incidents of one company affect other companies' stock prices in the same industry. After controlling the spillover effect, the resulting sample size is 78 firm-event observations.

The tool EVENTUS is used for the study. We examine two different possible time periods (windows) around the event date (denote as day 0) for the stock price reactions: (1) -1~+1, and (2) -30~+1, where -1 (-30) represents 1 day (30 days) *before* the event date and +1 stands for 1 day *after* the event date.[13] The first three-day period is the most popular time frame used in event studies, which focus on the immediate reaction of stock price around the event date assumed by the market efficient theory. However, we also look at a longer window period because we believe that, for security incidents, information leakage may be better captured through a longer period given the nature of security events. Based on the firm-event observations, we can calculate the abnormal return (AR) from the market model:

$$AR_{it} = R_{it} - \hat{\beta}_0 - \hat{\beta}_1 R_{mt} \qquad (2)$$

As shown by equation (2), abnormal return is the return that cannot be captured by the market as a whole or the ex post return over the event window minus the normal return. The average abnormal return (AAR_t) is defined as $(\sum_{i=1}^{N} AR_{it})/N$. The total effect of an economic event on stock price is reflected in mean cumulative abnormal return (MCAR), which is the summation of abnormal returns for company-event observations in the window we choose, i.e.

[13] We also checked the following three different windows: (1) -30~-1, (2) -7~+1, and (3) +1~+30, but we do not find any significant results.

$\left(\sum_{t=1}^{N}\sum_{t_0}^{t_1} AR_{it}\right)/N$, where t_0 and t_1 are the beginning and the ending trading day for the window we choose. For instance, if we choose the window (-1, +1), t_0 is one day before the event date and t_1 is one day after the event date. Cumulative abnormal return (CAR, $\sum_{t_0}^{t_1} AR_{it}$) for each observation is used for the cross-sectional analysis in the next section.

4.2.2 Cross-sectional analysis

In order to test our hypotheses, we formulate a cross-sectional analysis by regressing CAR calculated in the previous subsection on the measure of the number of disclosures in financial reports for both the experimental group and the control group. In addition to the variables for the measure of the number of disclosures, we introduce three control variables. First, we control for the industry effect. Industries are divided into two groups: business services (first two-digit SIC code is 73) and non-business services. This categorization is based on the following two reasons. First, it is based on the characteristics of the industry. We anticipate that companies with SIC code 73, such as Amazon.com and Microsoft, are more easily affected by security incidents. As a result, security related disclosures might play a more crucial role for these companies. Second, about 41% of the company in the experimental group is composed of the companies within the industry with SIC code 73, so it is necessary to control for the industry effect. The composition of our experimental group by industry is shown in Table 3.

Table 3. Composition of the Experimental Group by Industry

Industry (two-digit SIC code—name[a])	Percentage[b]	Industry (two-digit SIC code—name)	Percentage
20—Food and Kindred Products	0.93%	49—Electric, Gas, and Sanitary Services	0.93%
27—Printing, Publishing and Allied Industries	4.63%	59—Miscellaneous Retail	4.63%
28—Chemicals and Allied Products	0.93%	60—Depository Institutions	8.33%
30—Rubber and Miscellaneous Plastics Products	0.93%	61—Non-depository Credit Institutions	2.78%
35—Industrial and Commercial Machinery and Computer Equipment	6.48%	62—Security and Commodity Brokers, Dealers, Exchanges, and Services	2.78%
36—Electronic and Other Electrical Equipment and Components, except computer equipment	2.78%	70—Hotels, Rooming Houses, Camps, and Other Lodging Places	0.93%
37—Transportation Equipment	4.63%	73—Business Services	40.74%
40—Railroad Transportation	0.93%	78—Motion Pictures	1.85%
45—Transportation by Air	2.78%	79—Amusement and Recreation Services	0.93%
47—Transportation Services	0.93%	87—Services-Commercial Physical & Biological Research	0.93%
48--Communications	9.26%		

[a] See http://www.osha.gov/pls/imis/sic_manual.html for the name of different industries. [b] Calculated out of 108 observations

We also control for company size. Previous studies have shown that large firms are more able to endure shocks than small firms (Fama 1992). Large firms also invest more in security than small firms (PriceWaterhouseCoopers 2006). In order to control the size effect, we consider two different measures. Since there are several missing values of the market value of the equity from COMPUSTAT, we choose take the logarithm of a firm's net assets in the corresponding accounting period as a proxy for size. Furthermore, for our control group, we take the spillover effect into account by controlling the mean cumulative abnormal return of the industry during our windows.

Consequently, our models are as follows. First, we investigate whether the existence of the disclosures of information security related risk factors ($DSec_i$) is related to CAR using the full sample in Equation (3). Then we examine the relationship in detail with equation (4) and (5).

$$CAR_i = \beta_0 + \beta_1 Dins_i + \beta_2 Size_i + \beta_3 DSec_i + \beta_4 Trisk_i + \varepsilon_i \quad (3)$$

$$CAR_i = \beta_0 + \beta_1 Dins_i + \beta_2 Size_i + \beta_3 ConP_{1i} + \beta_4 ConP_{2i} + \beta_5 ConP_{3i} + \beta_6 Sec_i + \beta_7 Trisk_i + \varepsilon_i \quad (4)$$

$$CAR_i = \beta_0 + \beta_1 Dins_i + \beta_2 Size_i + \beta_3 ConP_i + \beta_4 Sec_i + \beta_5 Trisk_i + \varepsilon_i \quad (5)$$

where i: number of observations,

CAR: cumulative abnormal return (defined in 4.2.2)

Dins: dummy for industry, 1 for SIC code 73, 0 for other industries

Size: logarithm of a firm's net assets

$ConP_j$: one, if there is disclosure of control and procedures: evaluate, management, or change. *ConP* in equation (5) is the summation of $ConP_j$ for j =1~3.

Dsec: dummy variable for the disclosures of information security related risk factors. *Dsec* equals to 1 if there is disclosure; 0, otherwise.

Sec: logarithm of the number of information security related risk disclosures

Trisk: logarithm of total number of risk factors disclosed[14]

ε: residual term

Equations (4) and (5) allow us to examine the effect of the disclosure of internal control and procedures both by three different elements and by it as a whole. From our hypothesis, we expect β_3, β_3 to β_6, β_3 and β_4 to be negative in equation (3) to (5) for the experimental group.

We further estimate different models for a more detailed analysis. First, we use the whole sample set without considering the disclosures of internal control and procedures as in equation (6) where β_3 is expected to be negative. The effects of different types of incidents are also investigated in equation (7) where *DConf* and *DInt* are dummies for confidentiality type and integrity type incidents. For availability type of incidents, *DConf* and *DInt* are both set to be equal to zero.

$$CAR_i = \beta_0 + \beta_1 Dins_i + \beta_2 Size_i + \beta_3 Sec_i + \beta_4 Trisk_i + \varepsilon_i \quad (6)$$

$$CAR_i = \beta_0 + \beta_1 Dins_i + \beta_2 Size_i + \beta_3 Sec_i + \beta_4 Trisk_i + \beta_5 DConf_i + \beta_6 DInt_i + \varepsilon_i \quad (7)$$

Second, since companies started to disclose control and procedures after SOX, we also investigate the subsample *before* 2002 (hereafter referred to as subsample 1) for equation (6). Last, we use only the sample *after* 2002 (including 2002) (hereafter referred to as subsample 2) to estimate the impact of the full model as shown in equation (4) and (5). The above two analyses are performed in order to rule out possible systematic differences across time. We are also able to investigate the impact of the disclosures of internal control and procedures on CAR separately and aggregately, where β_3 to β_5 are expected to be negative in equation (8) and β_3 is expected to be negative in equation (9).

[14] We have checked whether the total number of risk factors can perfectly predict the number of information security related risk disclosures in order to rule out the possibility of multicollinearity. We do not see such result.

$$CAR_i = \beta_0 + \beta_1 Dins_i + \beta_2 Size_i + \beta_3 ConP_{1i} + \beta_4 ConP_{2i} + \beta_5 ConP_{3i} + \varepsilon_i \quad (8)$$

$$CAR_i = \beta_0 + \beta_1 Dins_i + \beta_2 Size_i + \beta_3 ConP_i + \varepsilon_i \quad (9)$$

Equations (4) to (9) (except equation (7)) are applied to both the experimental and the control group. For the control group, there are 40 observations for subsample 1 and 38 observations for subsample 2 after controlling the spillover effect.[15]

In order to empirically test our third hypothesis, we divide our sample of the experimental group into two groups. The matched group contains observations where the types of information security incidents match the disclosed information security risk factors. The other group, the unmatched group, has the observations where the types of information security incidents do not match the disclosed information security risk factors. For robustness, we apply three different measures for the variable *Match* in equation (10). The first measure is whether there exists a match (*DMatch*). The second measure, *PMatch*, is the percentage of the number of incidents that matches the number of information security risk factors (*Sec*). For example, a company experiences a DoS attack and such an incident is in one of the four possible risk factors disclosed. Then, *PMatch* equals to 25%. The third measure *NMatch* is the percentage of the number of incidents that matches the number of information security risk factors actually disclosed in the contents. For example, there are 20 possible information security risk factors disclosed in the contents and one of them matches the incident. Then, *NMatch* equals to 5%.[16]

$$CAR_i = \beta_0 + \beta_1 Dins_i + \beta_2 Size_i + \beta_3 Sec_i + \beta_4 Trisk_i + \beta_5 Match_i + \varepsilon_i \quad (10)$$

We further examine whether the mitigation effect is limited to first time disclosures. Disclosures are distinguished from acknowledgements. Disclosures are the first time

[15] For robustness of our results, we conduct the analysis under both unequal and equal number of observations across the experimental and the control group. Our main results shown in the next section remain the same.
[16] Since the disclosures of internal control and procedures are relatively standardized and cannot be matched to information security incidents, they are excluded from this analysis.

announcements. But acknowledgements are disclosures that have been released in previous years. Thus, we trace all our information security related risk disclosures back to 1997[17] (or as early as possible) and determine whether these pieces of information have been disclosed in previous years' financial reports. We first investigate if *any* of the disclosures have already been disclosed (*DPrev*). Next, the variable *Prev* is employed to capture the percentage of information security related risk disclosures that have been disclosed previously. For instance, for company A, there are four information security related risks factors disclosed in the event year. Two of them have been disclosed in previous years' reports. In this case, *Prev* is set to be 50%.[18] We add the variable to equation (6) and examine whether our previous results are affected.[19] That is

$$CAR_i = \beta_0 + \beta_1 Dins_i + \beta_2 Size_i + \beta_3 Sec_i + \beta_4 Trisk_i + \beta_5 DPrev_i + \varepsilon_i \quad (11)$$

$$CAR_i = \beta_0 + \beta_1 Dins_i + \beta_2 Size_i + \beta_3 Sec_i + \beta_4 Trisk_i + \beta_5 Prev_i + \varepsilon_i \quad (12)$$

It is expected that the coefficients of *DPrev* and *Prev* are non-positive.

4.2.3 Text mining

As mentioned, in order to better understand how expectations are formulated, we perform text mining on the disclosures. Text mining is the technique used to extract information from text. The information is extracted through finding nontrivial patterns and trends using tools such as statistical pattern learning (Tan 1999; Feldman and Sanger 2006). There are two major purposes of text mining: exploration and prediction (SAS Institute Inc 2004). Exploration or

[17] We pick the year 1997 because 1997 is roughly the year that the Internet starts to get popular. Before 1997, we can hardly get information security related disclosures. Furthermore, 1997 is the earliest year that we can retrieve financial reports from EDGAR Online for most of our observations.

[18] We also consider a more detailed coding scheme. For example, for those companies with non-zero *Prev* value, we further code the disclosure content into one of the three types of information security risks: confidentiality, integrity, and availability, and see how many (the percentage as *Prev*) of them have been disclosed. However, we found out that we do not need to consider whether the elements in each risk factor are the same or not because if the disclosures are the same, they will be exactly the same. Thus, a more complicated coding scheme does not provide us more information.

[19] The disclosures of internal controls and procedures are only available after year 2002. If we incorporate those disclosures in our regression, the resulting sample size becomes 17 observations, which might result in a biased estimation. More importantly, they are more like standardized disclosures. This analysis is not meaningful for them.

prescriptive mining enables us to discover the concepts from textual information and prediction or predictive mining allows us to use implicit information within the textual information for decision-making (SAS Institute Inc 2004). Text mining techniques have been widely used in different industries and different contexts, such as drug design in the medical industry or customer support (Fan et al. 2006; Han et al. 2002). For our study, by applying text mining techniques on the contents of the risk factor disclosures, we are able to identify and categorize the risk factors that are related to information security more specifically. The qualitative results can be used to explain the results in the cross-sectional analysis. Furthermore, as shown by the literature, how these risks are disclosed can affect the formation of expectations (Katz 2001).

The tool we use for text mining is SAS® 9.1 Text Miner which is embedded in Enterprise Miner. The analysis is performed in the following steps.

(1) The contents of information security related risk factors are used as inputs (documents).

(2) Text parsing decomposes the sentences into terms. In our study, we choose to rule out definite as well as indefinite articles, conjunctions, auxiliaries, prepositions, pronouns and interjections since these terms do not help provide meaningful results in our context.

(3) From the decomposition step, the Text Miner creates a frequency matrix as a quantitative representation of the input documents. The row vectors of this matrix represent the parsed terms in documents and the column vectors show the frequency of the terms, the number of documents the terms have shown and the weight for the terms. The weight for term i in document j (w_{ij}) is the multiplication of the frequency weight (L_{ij}) and the term weight (G_i). In our study, the frequency weight is the logarithm of the frequency (f_{ij}) of term i in document j plus one, i.e. $L_{ij} = \log_2 (f_{ij} + 1)$. The term weight of term i (G_i) is calculated as $1 + \sum_j \left(p_{ij} \log_2 \left(p_{ij}\right) / \log_2 (n)\right)$, where $p_{ij} = f_{ij} / g_{ij}$, f_{ij} is the frequency of term i in

document j, g_i is the number of times term i appears in the data set, and n is the number of documents in the data set. These two methods put more weights on words that show in few documents and generally give the best results (SAS Institute Inc 2004).

(4) For dimension reduction, we use the single value decomposition (SVD) method. SVD generates the dimensions that best represent the original frequency matrix. Through matrix factorization and projection[20], SVD forms the dimension-reduced matrix. The dimensions resulting from applying SVD depend on the resolution and maximum dimensions. The higher the resolution, the higher the SVD dimensions, which generally summarize the data better (SAS Institute Inc 2004). In our analysis, we set the maximum dimensions to be one hundred[21] (as default) and set the resolution to be low, medium, or high as a robustness check. The resulting SVD dimensions are further used for cluster analysis.

(5) We then divide our data into disjoint groups using expectation maximization clustering and set the maximum clusters to be forty (as default). The expectation maximization method is an iterative process that estimates the parameters in the mixture model probability density function[22] which approximates that data distribution by fitting k cluster density function to a data set. The iteration terminates if the likelihood value of two iterations is less than $\varepsilon > 0$ or a maximum of five iterations are reached (SAS Institute Inc 2004).

The text mining results are discussed in section 4.3.2.

---

[20] The singular value decomposition of a frequency matrix (A) is to factorize the matrix into matrices of orthonormal columns and a diagonal matrix of singular values, i.e. $A = U\Sigma V^T$. Then the original documents are projected to matrix U (SAS Institute Inc 2004).

[21] The maximum value of dimensions can at most be four less than the minimum of the number of rows and number of columns of the original frequency matrix (SAS Institute Inc 2004). Therefore, for our data (or documents), the maximum number of dimensions is definitely below one hundred.

[22] The mixture model probability density function evaluated at point x equals to $\sum_{h=1}^{k} \omega_h f_h(x|\mu_h, \Sigma_h)$, where μ_h, Σ_h are the mean vector and covariance matrix for cluster h under Gaussian probability distribution. For each observation x at iteration j, whether x belongs to a cluster h equals to $\left(\omega_h^j f_h(x|\mu_h^j, \Sigma_h^j)\right) / \left(\sum_i \omega_i^j f_i(x|\mu_i^j, \Sigma_i^j)\right)$ (SAS Institute Inc 2004).

4.3 Results

By applying the market model, we first examine the market reactions to information security incidents for both the experimental group and the control group. For the experimental group, the market reactions to the incidents are consistently and significantly negative for both time windows (-1, +1) and (-30, +1). Interestingly, for the control group the reaction is insignificantly positive for the short window and significantly negative for the long window.[23] This observation provides anecdotal evidence on the existence of the spillover effect and confirms the results shown by Ettredge and Richardson (2003). For companies in the control group, although they do not suffer from the incident, on average, there still exists a negative impact on business value given those incidents. This result further confirms the need to control for spillover effects for the control group.

4.3.1 Results for event study

We first examine whether the existence of the disclosures of information security related risk factors relates to CAR. Table 4 demonstrates that, for the experimental group, the existence of the disclosures of information security related risk factors is significantly and negatively related to CAR. But for the control group, there is no such result.

Table 4. Results for the Existence of the Disclosures of Information Security Risk Factors

Variables	Experimental Group		Control Group	
	Window (-1,+1)	Window (-30,+1)	Window (-1,+1)	Window (-30,+1)
Intercept	**-0.06****	-0.01	0.02	0.01
Dins	0.00	-0.05	0.01	0.01
Size	0.00	-0.01	0.00	0.00
DSec	**-0.03****	**-0.19****	0.00	-0.04
Trisk	**0.01****	0.05	-0.01	-0.04

* significant at 10% ** significant at 5% ***significant at 1%

[a] There are 90 observations for the experimental group and 80 observations for the control group.

[23] For the experimental group, the negative impacts (mean cumulative abnormal return, MACR) are -0.37% and -4.42% respectively. Further, the negative impact is significant (Patell Z = -1.322) for the thirty-two day window but insignificant (Patell Z= 0.837) for the three-day period. For the control group, there is a positive impact, 0.08%, for the period (-1, +1) (Patell Z = 0.749). But the impact is significantly negative, -3.79%, for the window (-30, +1) (Patell Z = -1.398).

The preliminary result in Table 4 can be further examined through the following analyses. Results using subsample 2 from the experimental group are shown in Table 5. Table 5 demonstrates that the impact of the disclosures of internal control and procedures and the number of information security related risk disclosures are not significant for most of the cases. But the impact of the disclosure of the evaluation of internal controls and procedures ($ConP_1$) is significantly positive. For the control group (Table 6), the results are not significant in the three-day window. However, the impact of the disclosure of the change of internal controls and procedures ($ConP_3$) is significantly negative in the long window. Furthermore, the total risk factors are significantly negative but the effect of company size is positive. We also do not observe the impact of spillover effects on CAR. Therefore, hypothesis 1 is not supported.

Table 5. Results for Model 4, 5, 8, and 9 using Subsample 2 for the Experimental Group[a]

Variables	Window (-1,+1)				Window (-30,+1)			
	Model 4	Model 5	Model 8	Model 9	Model 4	Model 5	Model 8	Model 9
Intercept	-0.07	-0.06	-0.03	-0.02	**-0.46****	**-0.38***	-0.26	-0.23
Dins	-0.02	-0.02	0.00	-0.01	-0.07	-0.09	0.00	-0.01
Size	0.00	0.00	0.00	0.00	0.01	0.01	0.01	0.01
Sec	0.00	0.00			0.02	0.04		
Trisk	0.02	0.02			**0.08***	0.07		
ConP		0.01		0.01		0.02		0.04
$ConP_1$	0.03		**0.03***		0.09		**0.12***	
$ConP_2$	0.02		0.02		0.11		0.12	
$ConP_3$	-0.02		-0.01		-0.07		-0.06	

* significant at 10% ** significant at 5% ***significant at 1%

[a] There are 37 observations in subsample 2 for the experimental group.

Table 6. Results for Model 4, 5, 8, and 9 using Subsample 2 for the Control Group[a]

Variables	Window (-1,+1)				Window (-30,+1)			
	Model 4	Model 5	Model 8	Model 9	Model 4	Model 5	Model 8	Model 9
Intercept	-0.01	0.00	0.01	0.02	0.15	0.13	-0.15	-0.06
Dins	0.01	0.01	0.01	0.01	0.05	0.05	0.02	0.02
Size	0.00	0.00	0.00	0.00	**0.03***	0.02	0.02	0.01
Sec	0.00	0.00		-0.01	-0.01	-0.03		
Trisk	0.01	0.01			**-0.16****	**-0.11***		
ConP		-0.01				-0.07		**-0.09****
$ConP_1$	0.00		0.00		0.00		0.00	
$ConP_2$	-0.01		-0.01		-0.01		-0.09	
$ConP_3$	-0.01		-0.01		**-0.12****		**-0.10***	
MCAR	1.48	1.48	1.49	1.41	0.58	0.65	0.63	0.63

* significant at 10% ** significant at 5% ***significant at 1%

[a] There are 38 observations in subsample 2 for the control group. Further, all companies in the control group provide information about evaluation of internal controls and procedures ($ConP_1$).

Several points are worth addressing. First, for breached firms, the disclosures of internal control and procedures do not impact CAR for most of the cases except the evaluation of internal controls ($ConP_1$) which is significant in Model 8. Since breached firms are suffering from the incidents, how these companies evaluate their internal controls becomes an important piece of information because such information can help investors determine the consequences of those incidents. However, interestingly, the coefficient is positive. We argue that this is because though companies disclose how they evaluate their internal controls and procedures, they still experience security incidents. Thus, such evaluation might cause an opposite image to investors thereby resulting in a positive relationship with CAR. For the control group, it seems that investors weigh more on the change in internal controls ($ConP_3$) for these companies. This is because any information regarding changes in internal control practices might inform investors about these companies' reactions to the incidents. Such information can help mitigate the impacts of information security incidents.

Second, company size is another important element for the control group. Company size (*Size*) significantly but positively affects CAR. The positive coefficient is different from the literature and seems counter intuitive at first glance. We argue that since bigger companies might become a target in the future, investors concern more about these companies even though they are not suffering from any incident now. That is why we observe a positive coefficient. Furthermore, for the control group, business risk factors (*Trisk*) significantly and negatively affect CAR. Because companies in the control group do not experience any incidents, general business environment and operation conditions are more relevant to these companies. Therefore, business risk factors describing the uncertainties a company faces in the business environment should convey important information about companies' future profitability to investors.

Third, for the experimental group, none of information security related disclosures has significant impacts on CAR. There are several possible reasons. First, the information contents of information security related disclosures are somehow overlapping or correlated with each other (e.g. Eihorn 2005). Therefore, the effect becomes unclear. Second, the disclosures of control and procedures are quite standardized and relatively inflexible. Also, the focus of the disclosures is mostly on regulation compliance. There is less "real" information content about possible future risks. Thus, financial report users might not be able to adjust expectation of business value from the disclosures of control and procedures. Last, the sample size is relatively small for subsample 2 (37 observations). A small sample size might also lead to the insignificant results.

We further examine the relationship between CAR and risk disclosures. The results are shown in Table 7. For the experimental group, no matter which time period we choose, the results consistently show that, as expected, the number of security related risk disclosures (*Sec*) significantly and negatively affects CAR. This finding supports our second hypothesis that the greater the number of information security related risk disclosures (*Sec*), the smaller the impact of information security incidents on stock prices. We demonstrate that the number of information security related disclosures indeed plays an important role in conveying information security risk to the market. Investors pay more attention on information security related disclosures for firms under attack because these disclosures help investors understand the impact of such incidents on the company. There are two points regarding our control variables in the experimental group worth noting here. First, the result from subsample 1 in Table 7 confirms that large firms face relatively smaller impacts than small firms, as suggested by previous studies (Fama and French 1992; PriceWaterhouseCoopers 2002). Second, we do not see that security

related disclosures impact the business services industry more than other industries. For the control group, as expected, the number of security related risk disclosures (*Sec*) does not significantly affect CAR.

Table 7. Results for Risk Factor Disclosures[a]

Variables	Window (-1,+1)				Window (-30,+1)			
	Experimental Group		Control Group		Experimental Group		Control Group	
	Full sample	Sub-sample 1	Full sample	Sub-sample 1	Full sample	Sub-sample 1	Full sample	Sub-sample 1
Intercept	**-0.05***	-0.03	0.02	0.06	0.04	0.64**	-0.01	0.07
Dins	0.00	0.01	0.00	0.01	-0.05	-0.01	0.01	0.03
Size	0.00	0.00	0.00	0.00	-0.01	**-0.07*****	0.01	0.02
Sec	**-0.02****	**-0.05*****	0.00	-0.05	**-0.14****	**-0.39*****	-0.04	-0.02
Trisk	**0.01****	0.01	-0.01	-0.02	0.04	0.03	-0.04	**-0.13****
MCAR			0.17	-0.74			0.43	0.64

* significant at 10% ** significant at 5% ***significant at 1%

[a] For the experimental group, there are 90 observations for the full sample and 53 observations for subsample 1. There are 78 observations for the full sample and 38 observations for subsample 1 for the control group.

When we control for different types of information security incidents, the results are demonstrated in Table 8. Again, the impact of the disclosures of information security risk factors on CAR is significantly negative and company size helps a company endure the shock of the incidents. Also, consistent with Campbell et al. (2003), Table 8 shows that confidentiality and integrity type incidents increase the impact on stock price reactions compared to availability type incidents. We argue that this is because both confidentiality and integrity type incidents have more direct and indirect impacts on customers as well as a company's future profitability and the impacts are more difficult to measure compared to availability type ones. For example, the direct and potential impacts are generally larger if a company loses customer data (confidentiality type) instead of not being able to perform online transactions for several hours (availability type). Therefore, confidentiality and integrity type incidents can enlarge the surprises on stock prices compared to availability type ones.

Table 8. Results for Risk Factor Disclosures for Different Types of Incidents[a]		
Variables	Window (-1,+1)	Window (-30,+1)
Intercept	**-0.05***	0.12
Dins	0.00	-0.03
Size	0.00	**-0.03****
Sec	**-0.02****	**-0.12***
Trisk	0.01*	0.04
DConf	0.02	**0.23*****
DInt	0.02	**0.22*****
* significant at 10% ** significant at 5% ***significant at 1% [a] For the experimental group, there are 84 observations.		

So far, we have only investigated the impacts of information security related disclosures on CAR. We have not yet considered the effect when the disclosed information security risk factors match the incidents. The results are given in Table 9.[24] First, interestingly, Table 9 shows that for the matched group, business risk factors positively and significantly affect CAR. We posit that this is another type of spillover effect across risk factors. Since information security risk factors are part of the set of business risk factors, once the information security risk is realized, investors might focus more on other risk factors. That is, whether the breached company can survive from the incident helps investors formulate the expectation of the possibility that other risk factors will also realize in the future. Second, different from our argument, Table 9 demonstrates that whether the type of incident matches the disclosed risk factor does not significantly affect the stock price reactions for most of the cases even the directions are as expected. However, this finding does not suggest that the disclosures are useless in terms of expectation formulation. Instead, we argue that the result points out an interesting way of how users consider risk factor disclosures. That is, financial report users do not actually take specific risk factors into account. Users care more about the impacts and the business units or subjects that are affected regardless of the specific risk factors. As long as the impacts are similar, the

[24] We have checked whether there exists any difference between the companies in these two groups. The major difference of the companies is that the matched companies are mainly in the industry with first two-digit SIC code 73 which has already been controlled for. Therefore, our results are not biased by the difference of the companies across groups.

risk factors provide similar information to the investors. For instance, both virus attacks and DoS attacks can result in a disruption of online services. We argue that users pay more attention on the overall impact, i.e. disruption of online services, rather than what causes it, i.e. virus or DoS attacks. Therefore, we do not observe a significant relationship when we match incidents to disclosures but a significant relationship when we investigate the disclosures of information security risk factors in general. This argument is further investigated in the text mining section. Based on these results, our third hypothesis is not supported.

Table 9. Results for the Matched or Unmatched Group using Full Sample[a]

Variables	Window (-1,+1)				Window (-30,+1)			
Intercept	**-0.06****	**-0.06****	**-0.06***	**-0.06***	-0.01	-0.02	-0.02	-0.04
Dins	0.00	0.00	0.00	0.00	-0.04	-0.05	-0.03	-0.03
Size	0.00	0.00	0.00	0.00	-0.01	-0.01	-0.01	0.00
Sec	0.00	-0.02	**-0.02***	-0.02	0.00	-0.09	-0.09	-0.07
Trisk	**0.01****	**0.01****	**0.01****	**0.01****	0.05	0.05	0.05	0.05
DMatch	**-0.04***				-0.21			
PMatch		-0.03				-0.18		
NMatch			-0.08	-0.12			-0.87	-1.30

* significant at 10% ** significant at 5% ***significant at 1%

[a] There are 90 observations for the experimental group. Our results remain the same if we exclude six two-type events. Furthermore, for the measure *NMatch*, two raters perform the coding task independently. As shown in the table, our main results hold.

For the above analyses, we treat all the disclosures as first time disclosures. Next, we distinguish disclosures from acknowledgements, which are disclosures that have been announced in previous years' reports. First, we only investigate the effect if *any* of the disclosures that have been disclosed before (*DPrev*) as shown in Table 10. The results demonstrate a significantly negative relationship if any of the disclosures have been announced before. Based on this preliminary result, we further name the observations that have non-zero information security related risk factors as subsample 3 and incorporate the variable *Prev* as mentioned. The results in Table 11 support our fourth hypothesis that as the percentage of information security related risk factors disclosed in previous years' financial reports increases, the impact of information security incidents on stock prices decreases. Since the expectation has been formed, the impact

on stock price reaction is lessened. Furthermore, the impact of current year's information security risk factors becomes smaller. Thus, our fourth hypothesis is supported.

Table 10. Results for the Existing of Acknowledgements[a]

Variables	Window (-1,+1)		Window (-30,+1)	
	Experimental Group	Control Group	Experimental Group	Control Group
Intercept	**-0.06***	0.03	0.03	0.01
Dins	0.00	0.00	-0.06	0.01
Size	0.00	0.00	-0.01	0.01
Sec	0.00	**0.08***	-0.02	0.06
Trisk	**0.01****	-0.01	0.05	-0.04
DPrev	**-0.05****	**-0.07****	**-0.21***	-0.09
MCAR		0.10		0.41

* significant at 10% ** significant at 5% ***significant at 1%
[a] For the experimental group, there are 90 observations. There are 78 observations for the control group.

Table 11. Results for Disclosures and Acknowledgements[a]

Variables	Window (-1,+1)				Window (-30,+1)			
	Experimental Group		Control Group		Experimental Group		Control Group	
	Full sample	Sub-sample 3	Full sample	Sub-sample 3	Full sample	Sub-sample 3	Full sample	Sub-sample 3
Intercept	**-0.06****	-0.14	0.03	-0.02	0.01	-0.16	0.01	0.08
Dins	0.00	0.01	0.00	0.05	-0.04	0.12	0.01	-0.07
Size	0.00	0.01	0.00	0.01	-0.01	0.01	0.01	0.05
Sec	-0.01	-0.02	**0.08***	0.22	-0.08	-0.01	0.06	0.15
Trisk	**0.01****	0.03	-0.01	-0.08	0.05	-0.01	-0.04	-0.26
Prev	**-0.05*****	**-0.06****	**-0.07****	-0.05	-0.15	-0.14	-0.09	-0.11
MCAR			0.10	5.79			0.41	-1.43

* significant at 10% ** significant at 5% ***significant at 1%
[a] For the experimental group, there are 90 observations for the full sample and 31 observations for subsample 3. There are 78 observations for the full sample and 13 observations for subsample 3 for the control group.

4.3.2 Cluster analysis results

In order to better understand how information security related risk factors form expectations in addition to the previous analyses, we perform text mining on the titles and contents of such factors. Table 12 demonstrates the clustering results on the titles (contents) under high, medium, and low resolutions. The result shows that the titles of information security related risk factors in the experimental group have already pointed out the impacts of such risks. If we further look into the key concepts provided by the contents, the contents also provide similar concepts as the titles thereby pointing out the negative impacts of those risk factors, such as disruption, interruption, and failure, and the subjects that may be affected, such as business, users, and

infrastructure. For the control group, similarly, the key concepts lie within the titles and contents show the negative impacts of those risk factors, such as failure, disruption, and interruption. The affected subjects can be business, product, and customers. The results from Table 12 also justify our coding scheme and the explanation for the insignificance of hypothesis 3. That is, the findings suggest that users are only able to get a whole picture of the disclosures and understand the possible impacts through the titles and contents. Therefore, Table 12 justifies our coding scheme that investors take the risk elements as a whole to infer the impacts of information security incidents. The results also support our argument that we do not observe a significant relationship when we match incidents to disclosures because financial report users do not actually take specific risk factors into account. Moreover, the disclosures are not similar qualitatively across the experimental group and the control group. Interestingly, the experimental group mentions issues about brand, reputation, and operating results which are not disclosed by the non-breached companies.

Also, consistent with the results shown in Table 2, companies in the experimental group disclose more information security risk factors than those in the control group. Furthermore, for companies in the experimental group, many of such factors disclosed currently have already been disclosed previously. It seems that the breached companies gradually increase the number of information security risk factors disclosed in financial reports. We argue that these companies might attempt to disclose possible information security risk factors they faced before or they are suffering in the current period in order to lower the impact. By performing the cluster analysis on different year groups, we further investigate whether the text mining results vary from year to year. The results are presented in Table 13. Terms from year 1999 to 2006 consistently demonstrate that failure, interruption and disruption are the possible impacts. Interestingly, after

year 2003, it seems that data and customer starts to become two possible affected subjects. This evidence somehow confirms that there is a shift from availability type incidents to integrity and confidentiality type ones. This finding also suggests that companies may want to discuss the impacts of integrity and confidentiality type incidents in more detail when evaluating and assessing risk factors in the future.

The text mining results for the media announcement are shown in Table 14. As expected, since site attacks and virus attacks are popular in our sample, these terms show up in the text mining results. Combined with the results in Table 12, these results demonstrate the relationship between incidents, subjects and possible impacts as a whole.

Table 12. Text Mining Results of the Information Security Related Risk Factors[a]							
Experimental Group				**Control Group**			
Terms	Freq.	Percentage	RMS Std.	Terms	Freq.	Percentage	RMS Std.
Titles							
Resolution: High							
+increase, liability, reputation, suffer, +system	12	18%	0.142	adversely, +affect, +breach, business, security	11	61%	0.287
+disruption, +error, harm, operating results, +problem	8	12%	0.135	advertising, cause, +disrupt, inventory, significantly	7	39%	0.237
business plan, execute, only, plan, usage	7	11%	0.130				
Resolution: Medium							
+affect, +interruption, reputation, suffer, +system	13	20%	0.171	+breach, data, materially, +reduce, security	8	44%	0.332
adverse, have, +risk, security, subject	8	12%	0.148	advertising, cause, inventory, +operation, significantly	5	28%	0.249
+brand, +breach, fraudulent, operating results, security	7	11%	0.188	communication, damage, information, interruption, +service	5	28%	0.271
Resolution: Low							
confidential, +customer, information, +risk, security	10	15%	0.183	advertising, cause, +disrupt, inventory, significantly	7	39%	0.326
+damage, +failure, harm, operating results, +service	8	12%	0.168	damage, harm, interruption, +product, +service	6	33%	0.175
capacity, +constraint, +increase, suffer, +system	8	12%	0.178				
+activity, fraudulent, site, +user, web	7	11%	0.197				
Contents							
Resolution: High							
+demand, infrastructure, internet, not, +product	10	15%	0.137	+failure, interruption, +loss, +service, +system	14	78%	0.262
+continue, +depend, +experience, internet, +provide	10	15%	0.131	+affect, +customer, +network, perceived, +product	4	22%	0.184
+event, +failure, +interruption, +loss, +result	7	11%	0.125				
Resolution: Medium							
+business, information, not, security, +service	29	45%	0.177	+business, +customer, +have, information, other	10	56%	0.275
+computer, +experience, +failure, +interruption, +result	16	25%	0.171	+disaster, power, +reduce, +service, +telecommunication	6	33%	0.267
+disruption, +interruption, +loss, +telecommunication, +system	15	23%	0.164				
Resolution: Low							
+depend, +experience, internet, not, +user	18	28%	0.173	+event, +have, +interruption, not, +service	8	44%	0.228
+disruption, +event, +interruption, +loss, +system	13	20%	0.171	+ business, cause, financial, +network, security	8	44%	0.092
+breach, information, prevent, reputation, security	12	18%	0.156				

[a] The descriptive terms for the titles and contents with frequency over the percentage of 10% (the highest two) are reported for the experimental (control) group. A term with the plus (+) sign represents a group of equivalent terms. The percentage equals to the frequency of a set of terms divided by the total frequency. The root mean squared standard deviation (RMS Std) for a cluster k equals to $\sqrt{W_k/[d(N_k-1)]}$, where W_k is the sum of the squared distances from the cluster mean to each document in cluster k, d is the number of dimensions, and N_k is the number of documents that belong to cluster k.

Table 13. Text Mining Results of the Information Security Related Risk Factors for Different Year Groups[a]								
Experimental Group								
Year Group	Terms	Freq.	Percentage	RMS Std.	Terms	Freq.	Percentage	RMS Std.
	Titles				**Contents**			
Resolution: High								
1997-1998	No disclosures				No disclosures			
1999-2000	able, business, provide, reputation, +system	13	68%	0.257	+experience, +have, +interruption, +provide, +service	10	53%	0.263
2001-2002	adverse, confidential, +failure, have, information	4	50%	0.057	+affect, +event, +failure, +operation, +system	6	75%	0.151
	business, +expose, liability, reputation, suffer	4	50%	0.252				
2003-2004	business, +failure, harm, +interruption, +result	15	79%	0.255	+failure, +interruption, +network, +product, +service	13	68%	0.240
2005-2006	+business, +disrupt, harm, operating, operating results	14	74%	0.259	data, +disruption, +experience, +failure, +have	11	58%	0.249
Resolution: Medium								
1997-1998	No disclosures				No disclosures			
1999-2000	+failure, harm, other, reputation, +system	9	47%	0.253	+experience, +interruption, +loss, +provide, +user	13	68%	0.291
2001-2002	adverse, confidential, +failure, have, information	4	50%	0.057	+affect, +event, +failure, +operation, +system	6	75%	0.151
	business, +expose, liability, reputation, suffer	4	50%	0.252				
2003-2004	+cause, +customer, +delay, information, +system	8	42%	0.303	+disruption, +failure, +interruption, +provider, +service	11	58%	0.267
2005-2006	+event, information, materially, +network, +risk	7	37%	0.304	+disruption, +event, +experience, +failure, +service	10	53%	0.255
Resolution: Low								
1997-1998	No disclosures				No disclosures			
1999-2000	+breach, +increase, operating, site, web	9	47%	0.168	+experience, +have, +interruption, +loss, +provide	11	58%	0.266
2001-2002	adverse, confidential, +failure, have, information	4	50%	0.057	+affect, +event, +failure, +operation, +system	6	75%	0.151
	business, +expose, liability, reputation, suffer	4	50%	0.252				
2003-2004	+disruption, harm, +product, +service, +technology	8	42%	0.240	adversely, +affect, +customer, other, +system	11	58%	0.299
2005-2006	harm, operating, operating results, reputation, +result	11	58%	0.332	data, +disruption, +experience, +failure, +service	9	47%	0.220
Control Group								
	Titles				**Contents**			
Resolution: High								
1997-2001	N/A				N/A			
2002-2006	+breach, business, data, harm, security	9	60%	0.335	+interruption, +loss, +service, +telecommunication, vulnerable	8	53%	0.284
Resolution: Medium								
1997-2001	N/A				N/A			
2002-2006	+disrupt, lose, materially, +operation, significantly	7	47%	0.285	+affect, +business, financial, have, security	8	53%	0.316
Resolution: Low								
1997-2001	N/A				N/A			
2002-2006	business, +failure, harm, +operation, +system	11	73%	0.401	+event, +facility, +interruption, +reduce, +service	7	47%	0.211

[a] The descriptive terms for the titles and contents with the largest frequency are reported for both groups. For experimental group, there is no disclosure in the year group 1997-1998. For the control group, there are only three disclosures in the year group 1997-2001 which are not enough to perform cluster analysis. Thus, the sign shows not applicable. A term with the plus (+) sign represents a group of equivalent terms. The percentage equals to the frequency of a set of terms divided by the total frequency. The root mean squared standard deviation (RMS Std) for a cluster k equals to $\sqrt{W_k/[d(N_k-1)]}$, where W_k is the sum of the squared distances from the cluster mean to each document in cluster k, d is the number of dimensions, and N_k is the number of documents that belong to cluster k.

Table 14. Text Mining Results of the News of Information Security Incidents			
Terms	Freq.	Percentage	RMS Std.
Resolution: High			
+computer, internet, +site, +system, web	31	38%	0.110
+customer, +have, +make, +not, ‘s	51	62%	0.110
Resolution: Medium			
+attack, +computer, +problem, +send, +system	29	35%	0.133
+customer, +hacker, +have, +not, +service,	27	33%	0.137
+hacker, +make, more, +site, web	14	17%	0.129
Resolution: Low			
+account, +customer, +have, information, +number	13	16%	0.143
+flaw, +hacker, +problem, +site, +user	12	15%	0.127
+do, +file, +send, +spread, +virus	9	11%	0.128

5. Conclusions and Discussion

This paper investigates whether information security related disclosures in financial reports could mitigate the impacts of information security incidents. We use two different measures for information security related disclosures. One is the disclosures of internal control and procedures mandated by SOX. The other one is the disclosures of risk factors. Based on the observations of information security incidents we obtain from 1997 to 2006, we regress cumulative abnormal return (CAR) of each event on the number of disclosures along with control variables for both the breached companies (experimental group) and the non-breached companies (control group). Our results do not provide enough evidence for the relationship between the disclosures of internal control and procedures and CAR. However, how companies evaluate their internal controls and procedures is significantly related to CAR for the experimental group. On the other hand, the disclosure of the change in internal controls and procedures is significant for non-breached companies. The findings also demonstrate that the disclosures of information security risk factors can statistically significantly lower the impact of information security incidents. After further investigating the argument of expectation formulation in detail, we find that the impact of information security incidents on stock price reactions does not depend on whether the incidents match the content of the disclosures. This is because financial users focus more on the impacts of the events instead of the specific type of

incidents. Furthermore, when there is a match, business risk factors can increase the impact because investors might reconsider the possibility of occurrence of those risk factors in addition to information security risk factors. Similar to Campbell et al. (2003), this paper shows that confidentiality and integrity types of incidents can worsen the impact comparing to availability type incidents since these two types of incidents generally cause more direct and indirect consequences not only to the users but also to the company. We also demonstrate that there indeed exists a difference between first time disclosures and acknowledgements, which are the disclosures that have been released before. If the information security risk factors have been disclosed in previous years' reports, they are still negatively related to CAR. But the effect of risk factors disclosed in current year's report becomes insignificant. Last, interestingly, company size is a double-edged sword for breached companies and non-breached companies. Breached companies can benefit from a large company size because it allows the company to react and resist the negative shock. However, a large company size might cause non-breached companies become a future target. The text mining results point out that the impacts and the affected units and subjects of information security incidents are reflected by the titles and contents of risk factors. The results also suggest that companies can consider the direct and indirect impacts of integrity and confidentiality type incidents in order to better assess information security risks and better convey to financial report users.

This research has implications to both researchers and practitioners. For researchers, our findings provide some explanations that can be considered when conceptualizing risk management strategies especially after the implementation of SOX. Since there is no perfect security strategy that can prevent information security incidents from occurring, it is important to properly manage the risk. Our findings demonstrate the effect of disclosures in financial reports

on mitigating the impact of information security events in terms of business value, which can be considered part of a firm's risk management strategies. Though we may not be able to lower the likelihood of an event, it is possible to lessen the surprise through managing investors' expectations. Furthermore, our results show the importance of business risk factors for non-breached companies. For daily operations, these risk factors convey important information for investors and can be used for estimating the impacts on those companies. This paper also demonstrates possible issues in the literature of voluntary disclosure. As shown by the differences between the disclosure practices across our experimental and control group, there might be a different equilibrium disclosure practice than the ones discussed in the literature. More importantly, there can be some additional company characteristics or market impacts that lead to different disclosure practices.

For practitioners, the results shed light on how they can convey security practices to their customers more effectively. We observe that standardized disclosures of information security related issues provide relatively little information. It is not difficult to tell that the information those disclosures provide is meant to satisfy the requirements of SOX as opposed to voluntary disclosures. By properly reflecting possible security concerns, a company should be able to lower investors' sensitivity to information security incidents that a company might face in the future. Managers can also disclose possible information security related risk factors and their associated impacts in financial reports. By doing so, investors might discount the impacts of such events since they have formed expectations that these risks are embedded in daily operations. Moreover, when companies try to generate the disclosing information, executives should also consider the effectiveness of information security governance. That is, the company can at the same time identify the existing and emerging risk factors and assess the impact of such

factors. Based on the identification and assessment, executives are able to evaluate whether the current information security policies and practices are adequate and convey some of the information to investors for business value evaluation and investment decisions. Last, although our results do not focus on the impact of spillover effect and do not find it significant on CAR, our preliminary results demonstrate the control group might also be affected. Therefore, when considering the possible impacts of information security incidents, managers also need to take other companies effect into account. Moreover, companies in the same industry can also cooperate to mitigate the possible impacts of information security incidents.

There are several research limitations. One of the major limitations of our study is sample size. Although we attempt to capture as large of a sample as possible, it is still problematic to collect a larger data set base on our filtering processes and our research questions. A larger data set allows us to get different perspective of the text mining results from different industries. Also, many companies might suffer from information security incidents that are not disclosed to the public. Obviously, we are unable to incorporate this information into our sample. Second, we implicitly assume that the stock price truly reflects a company's business value. Although the stock price for high-tech companies might be biased, we only look at the price change in a short time period. Thus, we believe that our results still hold even with this possibility. Third, we adopt a simple coding scheme for the disclosures. Even though we believe that a more complicated coding scheme does not alter our main results, a finer coding scheme for all the disclosures that can be applied to different industries may provide the explanation in more detail.

Possible future extensions are as follows. First, in our paper, we implicitly assume that the disclosures are creditable and truly reflect a company's practices. However, some companies might disclose lots of information but invest little in reality. On the other hand, some other

companies might invest a lot of resources in information security but refuse to disclose to the public. Therefore, this anomaly is worth further investigation. Second, a larger data set can be used to provide more meaningful text mining results for both information security risk factors and business risk factors. The text mining analysis of business risk factors can also provide a first glance on how these risks affect different businesses. Third, as different media becomes popular information sources for investors, we can further consider other media sources, such as blogs, to investigate the relationship among different information sources, information security incidents, and stock price reactions. Last, the spillover effect can be investigated in detail by considering how the information is transferred and the major factors that result in the spillover effect.

Reference

Ajinkya, B. B., M. J. Gift. 1984. Corporate managers' earnings forecasts and symmetrical adjustments of market expectations. *J. of Accounting Res.* **22**(2) 425-444.

Amir, E., B. Lev. 1996. Value-relevance of nonfinancial information: the wireless communication industry. *J. of Accounting and Econom.* **22**(1-3) 3-30.

Baginski, S., E. Conrad, J. Hassell. 1993. The effects of management forecast precision on equity pricing and on the assessment of earnings uncertainty. *The Accounting Rev.* **68** 913-927.

Barron, O. E., C. O. Kile, T. B. O'Keefe. 1999. MD&A quality as measured by the SEC and analysts' earnings forecasts. *Contemporary Accounting Res.* **16**(1) 75-109.

Borge, D. 2001. *The book of risk*, NY: John Wiley& Sons, Inc.

Botosan, C. A. 1997. Disclosure level and the cost of equity capital. *The Accounting Rev.* **72**(3) 323-349.

Bowen, P., J. Hash, M. Wilson. 2006. *Information security handbook: a guide for managers*, NIST Special Publication 800-100.

Campbell, K., L. A. Gordon, M. P. Loeb, L. Zhou. 2003. The economic cost of publicly announced information security breaches: empirical evidences from the stock market. *J. of Computer Security* **11** 431-448.

Cavusoglu, H., B. Mishra, S. Raghunathan. 2004. The effect of internet security breach announcements on market value of breached firms and internet security developers. *Internat. J. of Electronic Commerce* **9**(1) 69-105.

CERT. 2007. *CERT/CC Statistics 1988-2006*, Retrieved Apr. 9 2007, from http://www.cert.org/stats/cert_stats.html.

CSI/FBI. 2007. *The CSI/FBI computer crime and security report in 2006*, Retrieved Apr. 9 2007, from http://abovesecurity.com/doc/CommuniquesPDF/FBISurvey2006.

Darrough, M. N. 1993. Disclosure policy and competition Cournot vs. Bertrand. *The Accounting Rev.* **68**(3) 534-561.

Dye, R. A. 1985. Disclosure of Nonproprietary Information. *J. of Accounting Res.* 12(1) 123-145.

Eihorn, E. 2005. The nature of the interaction between mandatory and voluntary disclosures. *J.of Accounting Res.* **43**(4) 593-621.

Elliott, R., P. Jacobson. 1994. Costs and benefits of business information disclosure. *The Accounting Horizons* **8**(4) 80-96.

Ettredge, M. L., V. J. Richardson. 2003. Information transfer among internet firms: the case of hacker attacks. *J.of Inform. Systems* **17**(2) 71-82.

Fama, E. 1970. The behavior of stock market prices. *J. of Finance* **25** 383–417.

Fama, E., K. French. 1992. The cross-section of expected stock returns. *J. of Finance* **47**(2) 427–465.

Fan, W., L. Wallace, S. Rich, Z. Zhang. 2006. Tapping the power of text mining. *Comm. of the ACM* **49**(9) 77-82.

Feldman, R., J. Sanger. 2006. *The text mining handbook: advanced approaches in analyzing unstructured data*, UK: Cambridge University Press.

Frame, J. D. 2003. *Managing risk in organizations: a guide for managers*. CA: Jossey-Boss.

Francis, J., K. Schipper, L. Vincent. 2002. Expanded disclosures and the increased usefulness of earnings announcements. *The Accounting Rev.* **77**(3) 515-546.

Focardi, S., C. Jonas. 1998. *Risk management framework, methods, and practice*, NJ: FJF Associates.

Foster, G. 1981. Intra-industry information transfers associated with earnings releases. *J. of Accounting and Econom.* **3**(3) 201-232.
Gal-Or, E., A. Ghose. 2005. The economic incentives for sharing security information. *Inform. Systems Res.* **16**(2) 186-208.
Garg, A., J. Curtis, H. Halper. 2003. Quantifying the financial impact of IT security breaches. *Inform. Management & Computer Security* **11**(2) 74-83.
Glover, S., S. Liddle, D. Prawitt. 2001. *Electronic commerce: security, risk management, and control*, NL: Prentice Hall.
Gordon, L. A., M. P. Loeb. 2002. The economics of information security investment. *ACM Transac. on Inform. and System Security* **5**(4) 438-457.
Gordon, L. A., M. P. Loeb, W. Lucyshyn. 2003. Sharing information on computer systems security: an economic analysis. *J.of Accounting and Public Policy* **22**(6) 461-485.
Gordon, L. A., M. P. Loeb, W. Lucyshyn, R. Richardson. 2005. *Tenth annual CSI/ FBI computer crime and security survey*. Computer Security Institute, 1-26.
Gordon, L. A., M. P. Loeb, W. Lucyshyn, T. Sohail. 2006. The impact of the Sarbanes-Oxley Act on the corporate disclosures of information security activities. *J. of Accounting and Public Policy* **25** 503-530.
Grossman, S. J. 1981. The information role of warranties and private disclosure about product quality. *J. of Law and Econom.* **24**(3) 461-483.
Healy, P. M., K. G. Palepu. 2001. Information asymmetry, corporate disclosure, and the capital markets: a review of the empirical disclosure literature. *J. of Accounting and Econom.* **31**(1-3) 405-440.
Hovav, A., J. D'Arcy. 2003. The impact of denial-of-service attack announcements on the market value of firms. *Risk Management and Insurance Rev.* **6**(2) 97-121.
Han, J., R. Altman, V. Kumar, H. Mannila, D. Pregibon. 2002. Emerging scientific applications in data mining. *Comm. of the ACM* **45**(8) 54-58.
Kannan, K., J. Rees, S. Sridhar. 2007. Market reactions to information security breach announcements: an empirical study. *Internat. J. of Electronic Commerce*, forthcoming.
Katz, S. B. 2001. Language and persuasion in biotechnology communication with the public: How not to say what you're not going to say and not say it, *AgBioForum* **4**(2) 93-97.
King, R., G. Pownall, G. Waymire. 1990. Expectations adjustment via timely management forecasts: review, synthesis, and suggestions for future research. *J. of Accounting Lit.* **9** 113-144.
Lang, M. H., R. J. Lundholm. 1993. Cross-sectional determinants of analyst ratings of corporate disclosures. *J. of Accounting Res.* **31** 216-271.
Lang, M. H., R. J. Lundholm. 1996. Corporate disclosure policy and analyst behavior. *The Accounting Rev.* **71**(4) 467-492.
Landsman, W., E. Maydew. 2002. Has the information content of quarterly earnings announcements declined in the past three decades? *J. of Accounting Res.* **40**(3) 797-807.
Lev, B., S. H. Pennman. 1990. Voluntary forecast disclosure, nondisclosure, and stock prices. *J. of Accounting Res.* **28**(1) 49-76.
Li, F. 2006. Annual report readability, current earnings, and earnings persistence. Working Paper, University of Michigan.
MacKinlay, A. C. 1997. Event studies in economics and finance. *J. of Econom. Lit.* **35**(1) 13-39.
Milgrom, P. R. 1981. Good News and Bad News: Representation Theorems and Applications. *Bell J. of Econom*. **12**(2) 380-391.

Penno, M. 1997. Information quality and voluntary disclosure. *The Accounting Rev.* **72**(2) 275-284.

Pownall, G., C. Wasley, G. Waymire. 1993. The stock price effects of alternative types of management earnings forecasts. *The Accounting Rev.* **68** 896-912.

PriceWaterhouseCoopers. 2002. *Inform. Security Breaches Survey 2002 – A Technical Re*port. Prepared by PriceWaterhouseCoopers for the Department of Trade and Industry.

Sandhu, R., E. Coyne, H. Feinstein, C. Youman. 1996. Role based access control models. *IEEE Comput.* **29**(2) 38-47.

Sandoval, G., T. Wolverton. 2000. Leading web sites under attack. Retrrieved April 17, 2007, from http://news.com.com/Leading+Web+sites+under+attack /2100-1017_3-236683.html.

SAS Institute Inc. 2004. *Getting started with SAS® 9.1 text miner*. Cary, NC: SAS Institute Inc.

Skinner, D. J. 1994. Why firms voluntarily disclose bad news. *J. of Accounting Res.* **32**(1) 38-60.

Sohail, T. 2006. *To tell or not to tell: market value of voluntary disclosures of information security activities*. Unpublished doctoral dissertation, University of Maryland, Maryland.

Stocken, P. 2000. Credibility of voluntary disclosure. *RAND J. of Econom.* **31**(2) 359-374.

Tan, A. H. 1999. Text mining: the state of the art and the challenges. *Proc. of the PAKDD'99 Workshop on Knowledge discovery from Advanced Databases*, Beijing.

Tran, K., R. L. Rundle. 2000. Hackers attack major internet sites, cutting off Amazon, Buy.com, eBay. The Wall Street Journal. Retrieved March 2, 2007, from FACTIVA database.

Warren, M. J., W. E. Hutchinson. 2000. Cyber attacks against supply chain management systems. *Internat. J. of Physical Distribution and Logistics Management* **30** 710-716.

Verrecchia, R. E. 1983. Discretionary disclosure. *J. of Accounting and Econom.* **5**(3) 179-194.

Verrecchia, R. E. 2001. Essays on disclosures. *J. of Accounting and Econom.* **32**(1-3) 97-180.

Appendix A. Glossary of Terms

Term	Definition
Management Assessment of Internal Controls (or Internal Control Report or Disclosures of Control and Procedures)	According to SOX Section 404, the internal control report should: "(1) state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting, and (2) contain an assessment, as of the end of the most recent fiscal year of the issuer, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting." Source: http://news.findlaw.com/hdocs/docs/gwbush/sarbanesoxley072302.pdf
Internal Control	COSO Definition of Internal Control "Internal control is a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories: • Effectiveness and efficiency of operations • Reliability of financial reporting • Compliance with applicable laws and regulations Key Concepts • Internal control is a process. It is a means to an end, not an end in itself. • Internal control is effected by people. It's not merely policy manuals and forms, but people at every level of an organization. • Internal control can be expected to provide only reasonable assurance, not absolute assurance, to an entity's management and board. • Internal control is geared to the achievement of objectives in one or more separate but overlapping categories." Source: http://www.coso.org/key.htm
Cost of Capital	"The cost of capital for a firm is a weighted sum of the cost of equity and the cost of debt." Source: http://en.wikipedia.org/wiki/Cost_of_capital
Abnormal Return and Cumulative Abnormal Return	As shown by equation (2) on page 19, abnormal return is the return that cannot be captured by the market as a whole. The total effect of a certain event is reflected in cumulative abnormal return (CAR), which is the summation of abnormal returns for a certain company-event observation in the window we choose.
Accounting Period	"The time period assumption states that the economic life can be divided into artificial time period, e.g. month, quarter, year." Source: Kieso, D. E., Weygandt, J. J. & Warfield, T. D. (2001) *Intermediate Accounting* (10^{th} ed.) NJ: Wiley.

Appendix B. An Example of the Disclosures of Internal Control and Procedures

Excerpt from Yahoo's annual report for year 2005, retrieved on Apr.23, 2007
source: http://www.sec.gov/Archives/edgar/data/1011006/000110465906014033/a06-3183_110k.htm

"Evaluation of Disclosure Controls and Procedures

The Company's management, with the participation of the Company's principal executive officer and principal financial officer, has evaluated the effectiveness of the Company's disclosure controls and procedures (as such term is defined in Rules 13a-15(e) and 15d-15(e) under the Securities Exchange Act of 1934, as amended (the "Exchange Act") as of the end of the period covered by this report. Based on such evaluation, the Company's principal executive officer and principal financial officer have concluded that, as of the end of such period, the Company's disclosure controls and procedures are effective in recording, processing, summarizing and reporting, on a timely basis, information required to be disclosed by the Company in the reports that it files or submits under the Exchange Act.

Management's Report on Internal Control Over Financial Reporting

The Company's management is responsible for establishing and maintaining adequate internal control over financial reporting as defined in Rules 13a-15(f) and 15d-15(f) under the Exchange Act. Under the supervision and with the participation of the Company's management, including its principal executive officer and principal financial officer, the Company conducted an evaluation of the effectiveness of its internal control over financial reporting based on criteria established in the framework in Internal Control—Integrated Framework issued by the Committee of Sponsoring Organizations of the Treadway Commission. Based on this evaluation, the Company's management concluded that its internal control over financial reporting was effective as of December 31, 2005.

Because of its inherent limitations, internal control over financial reporting may not prevent or detect misstatements. Also, projections of any evaluation of effectiveness to future periods are subject to the risks that controls may become inadequate because of changes in conditions, or that the degree of compliance with the policies or procedures may deteriorate.

The Company's independent registered public accounting firm has audited management's assessment of the effectiveness of the Company's internal control over financial reporting as of December 31, 2005 as stated in their report which appears on page 58.

Changes in Internal Control Over Financial Reporting

There have not been any changes in the Company's internal control over financial reporting (as such term is defined in Rules 13a-15(f) and 15d-15(f) under the Exchange Act) during the most recent fiscal quarter that have materially affected, or are reasonably likely to materially affect, the Company's internal control over financial reporting."

Appendix C. Examples of Risk Factors

Excerpt from Amazon's annual report for year 2000, retrieved on Apr.23, 2007
source: http://www.sec.gov/Archives/edgar/data/1018724/000103221001500087/0001032210-01-500087.txt

"We Face Intense Competition

The e-commerce market segments in which we compete are relatively new, rapidly evolving and intensely competitive. In addition, the market segments in which we participate are intensely competitive and we have many competitors in different industries, including the Internet and retail industries.

Many of our current and potential competitors have longer operating histories, larger customer bases, greater brand recognition and significantly greater financial, marketing and other resources than we have. They may be able
to secure merchandise from vendors on more favorable terms and may be able to adopt more aggressive pricing or inventory policies. They also may be able to devote more resources to technology development and marketing than us.

As these e-commerce market segments continue to grow, other companies may enter into business combinations or alliances that strengthen their competitive positions. We also expect that competition in the e-commerce market segments will intensify. As various Internet market segments obtain large, loyal customer bases, participants in those segments may use their market power to expand into the markets in which we operate. In addition, new and expanded Web technologies may increase the competitive pressures on online retailers. The nature of the Internet as an electronic marketplace facilitates competitive entry and comparison shopping and renders it inherently more competitive than conventional retailing formats. This increased competition may reduce our operating profits, or diminish our market segment share."

"System Interruption and the Lack of Integration and Redundancy in Our Systems May Affect Our Sales

Customer access to our Web sites directly affects the volume of goods we sell and thus affects our net sales. We experience occasional system interruptions that make our Web sites unavailable or prevent us from efficiently fulfilling orders, which may reduce our net sales and the attractiveness of our products and services. To prevent system interruptions, we continually need to: add additional software and hardware; upgrade our systems and network infrastructure to accommodate both increased traffic on our Web sites and increased sales volume; and integrate our systems.

Our computer and communications systems and operations could be damaged or interrupted by fire, flood, power loss, telecommunications failure, break-ins, earthquake and similar events. We do not have backup systems or a formal disaster recovery plan, and we may have inadequate insurance coverage or insurance limits to compensate us for losses from a major interruption. Computer viruses, physical or electronic break-ins and similar disruptions
could cause system interruptions, delays and loss of critical data and could prevent us from providing services and accepting and fulfilling customer orders. If this were to occur, it could damage our reputation."

Appendix D. Sample

Company	Control Company	Event Date	Type of Incident	Financial Report Data Used
Aastrom Bioscience	Baxter International	2000/2/18	phony info[i]	10-K,2000
About.com		2000/2/10	site attack[a]	10-Q(1Q,2000)
Akamai tech	Blue Coat System	2004/6/16	site attack[a]	10-K,2004
Amazon.com	Barnes and Noble	2000/2/8	DOS[a]	10-K,2000
Amazon.com	Barnes and Noble	2000/2/9	DOS[a]	10-K,2000
Amazon.com	Barnes and Noble	2000/2/10	DOS[a]	10-K,2000
American express	Capital One	2003/2/19	hack info[c]	10-K,2003
AOL	EarthLink	2000/6/18	break in[c]	10-K,2000
AOL Times Warner	Walt Disney	2002/1/3	hole discovery[c]	10-K,2002
AOL Times Warner	Walt Disney	2006/8/22	breach[c]	10-K,2006
AT&T	Sprint	1999/6/10	worms[i]	10-K,1999
AT&T	Sprint	2006/8/24	online theft[c]	10-K,2006
AT&T	Sprint	2006/8/30	online theft[c]	10-K,2006
Bank of America	US Bancorp	1999/11/30	virus[i]	10-K,1999
Bank of America	US Bancorp	2003/2/6	worms[ia]	10-K,2003
Bank of America	US Bancorp	2005/2/28	data lost[c]	10-K,2005
Bank of America	US Bancorp	2006/3/13	breach[c]	10-K,2006
Boeing	Northrop Grumman	1999/6/10	worms[i]	10-K,1999
Boeing	Northrop Grumman	2003/1/28	worms[a]	10-K,2003
ChoicePoint	ISCO International	2005/2/22	ID theft[c]	10-K,2005
Cisco	Avaya	2004/5/18	code theft[c]	10-K,2004
Cisco	Avaya	2005/5/10	code theft[c]	10-K,2005
Citigroup	JPMorgan Chase	2006/3/8	breach[c]	10-K,2006
Citigroup	JPMorgan Chase	2006/3/13	breach[c]	10-K,2006
Coca Cola	Pepsi	1997/9/15	attack[a]	10-K,1997
Compaq	Gateway	1999/3/30	virus[i]	10-K,1999
Compaq	Gateway	2001/2/15	attack[a]	10-K,2001
Continental Airlines	AMR	2003/2/6	worms[i]	10-K,2003
Countrywide Financial	Fannie Mae	2003/1/28	attack[a]	10-K,2003
Cox Communications		2001/8/8	virus[i]	10-K,2001
Critical Path	Sun Micro	1999/9/22	breach[c]	10-K,1999
CSX	Norfolk Southern	2003/8/21	virus[i]	10-K,2003
Dell	IBM	1999/11/19	virus[i]	10-K,1999
Dell	IBM	2002/12/11	site crashed[a]	10-K,2002
Direct TV	EchoStar Communication	2003/1/3	data theft[c]	10-K,2003
Doubleclick	ValueClick	2001/3/30	attack[a]	10-K,2001
Doubleclick	ValueClick	2004/7/28	attack[a]	10-K,2004
Drug Emporium	Drug Store Com Inc.	2000/1/30	site shutdown[c]	10-K,2000
eBay		2000/2/8	DOS[a]	10-K,2000
eBay		2000/2/9	DOS[a]	10-K,2000
eBay		2000/2/10	DOS[a]	10-K,2000
Estee Lauder	Procter and Gamble	2000/5/5	virus[ia]	10-K,2000
FedEx	UPS	2001/8/9	virus[a]	10-K,2001
First Data Corp	Fiserv	2000/9/11	break in[c]	10-K,2000
Ford Motor	General Motor	2000/5/5	virus[ia]	10-K,2001
Ford Motor	General Motor	2005/12/22	data lost[c]	10-K,2005
Ford Motor Credit		2002/5/17	hack credit info[c]	10-K,2003
General Electric	Philips Electronics	1999/6/10	worms[i]	10-K,1999
Google	eBay	2004/7/27	virus[i]	10-K,2004
Hilton	Marriot International	2005/5/20	breach[c]	10-K,2005

[c]Confidentiality, [i]Integrity, [a]Availability

Company	Control Company	Event Date	Type of Incident	Financial Report Data Used
Hewlett Packard	IBM	2001/2/15	attack[a]	10-K,2001
Intel	AMD	1999/3/30	virus[i]	10-K,1999
Intel	AMD	1999/6/10	worms[i]	10-K,1999
Knight Ridder	Pulitzer	2003/9/10	attack[a]	10-K,2003
Lockheed Martin	Northrop Grumman	1999/3/30	virus[i]	10-K,1999
Mastercard		2003/2/19	hack info[c]	10-K,2003
Mastercard	American Express	2005/6/19	attack[c]	10-K,2005
McGraw-Hill	Moodys	2000/2/22	theft of data[c]	10-K,2000
MCI WorldCom	Nextel	1998/12/21	virus[i]	10-K,1998
MCI WorldCom	Nextel	1999/6/18	virus[i]	10-K,1999
MCI WorldCom	Nextel	2001/12/6	security breach[c]	10-K,2001
Merrill Lynch	Goldman Sachs	1999/3/30	virus[i]	10-K,1999
Microsoft	IBM	1997/6/23	hacker[a]	10-K,1997
Microsoft	IBM	1999/3/30	virus[i]	10-K,1999
Microsoft	IBM	1999/6/10	worms[i]	10-K,1999
Microsoft	IBM	1999/8/31	attack[a]	10-K,2000
Microsoft	IBM	2000/10/27	attack[c]	10-K,2001
Microsoft	IBM	2000/11/8	attack[c]	10-K,2001
Microsoft	IBM	2001/1/25	DOS[a]	10-K,2001
Microsoft	IBM	2001/1/26	DOS[a]	10-K,2001
Microsoft	IBM	2001/8/10	worms[i]	10-K,2002
Microsoft	IBM	2001/8/30	breach[c]	10-K,2002
Microsoft	IBM	2001/11/3	breach[c]	10-K,2002
Microsoft	IBM	2001/11/5	breach[c]	10-K,2002
Microsoft	IBM	2002/8/23	breach[c]	10-K,2003
Microsoft	IBM	2003/8/15	worms[ia]	10-K,2004
Microsoft	IBM	2004/2/13	code lost[c]	10-K,2004
Microsoft	IBM	2004/4/14	breach[i]	10-K,2004
Microsoft	IBM	2004/6/26	breach[c]	10-K,2004
Microsoft	IBM	2006/10/13	breach[i]	10-Q(2Q,2007)
National Discount Brokers		2000/2/25	site attack[a]	10-Q(1Q,2000)
Network solutions		1999/7/3	site attack[a]	10-K,1999
New York Times	Dow Jones	1998/9/14	attack[a]	10-K,1998
New York Times	Dow Jones	2002/7/12	deface[a]	10-K,2002
Nike		2000/6/22	site attack[a]	10-K,2000
Sabre		2000/6/24	breach[c]	10-K,2000
SBC		1999/6/10	worms[i]	10-K,1999
SCO	IBM	2003/12/15	attack[a]	10-K,2003
SCO	IBM	2004/2/2	virus[i]	10-K,2004
SCO	IBM	2004/11/29	deface[a]	10-K,2004
Siebel	PeopleSoft	2003/1/24	worm[a]	10-K,2003
Southern Company	Unisource Energy	1999/6/10	worm[i]	10-K,1999
Symantec	McAfee	1999/6/10	worm[i]	10-K,1999
TD Ameritrade	Charles Schwab	2006/10/24	hack in account[c]	10-Q(1Q,2007)
T-mobile (Deutsche Telekom AG)	Sprint	2005/1/13	hack in account[c]	20-F, 2005
ToysRus		1999/11/8	site crashed[a]	10-K,1999
TransWorldAirlines	SkyWest	2000/3/21	Security breach[c]	10-Q(1Q,2000)
USA Today (Gannett)	Tribune	2002/7/12	deface[a]	10-K,2002
Verisign	Entrust	2002/3/21	site attack[a]	10-K,2002
Walt Disney	CBS	2000/9/27	DOS[a]	10-K,2000
Washington Mutual	Wachovia	2003/2/6	worm[ia]	10-K,2003
Wells Fargo	US Bancorp	2006/3/13	breach[c]	10-K,2006
Yahoo		2000/1/11	disruption[a]	10-K,2000

[c]Confidentiality, [i]Integrity, [a]Availability

Company	Control Company	Event Date	Type of Incident	Financial Report Data Used
Yahoo		2000/2/8	DOS[a]	10-K,2000
Yahoo		2000/2/9	DOS[a]	10-K,2000
Yahoo		2000/2/10	DOS[a]	10-K,2000
Yahoo		2004/7/27	virus[i]	10-K,2004
Yahoo	Google	2005/3/24	phisher[c]	10-K,2005

[c]Confidentiality, [i]Integrity, [a]Availability