Decision Support Systems 50 (2011) 651–661

Contents lists available at ScienceDirect

Decision Support Systems

journal homepage: www.elsevier.com/locate/dss

Firms' information security investment decisions: Stock market evidence of investors' behavior

Sangmi Chai [a], Minkyun Kim [b,*], H. Raghav Rao [c]

[a] Division of Business Administration, College of Business, Sangmyung University, Korea
[b] Department of Business Management and Economics, College of Social Science, Dongduk Women's University, Korea
[c] Department of Management Science & Systems, School of Management, SUNY at Buffalo, United States

ARTICLE INFO

Available online 19 August 2010

Keywords:
Information security investment
Market value
Event methodology
Abnormal returns
Investors' behavior
Sarbanes–Oxley Act (SOX)

ABSTRACT

In the information society, it is important for firms to manage their core information resources securely. However, the difficulty of measuring the return on an IT security investment is one of the critical obstacles for firms in making such investment decisions. By utilizing event methodology, this study examines the value of an investment in IT security, based on stock market investors' behavior toward a firms' IT security investment announcements. Based on a sample of 101 investment announcements of firms whose stocks are publicly traded in the U.S. stock market between 1997 and 2006, we find substantial support for the hypotheses that information security investment leads to positive abnormal returns for firms. Interestingly, security investments with commercial exploitation tend to result in higher returns than those for IT security improvement. Another interesting finding is that stock market reaction to security investments shows higher abnormal returns after the Sarbanes–Oxley Act (SOX) than any of those before it.

1. Introduction

In examining the recent business environment, the Internet is a critical infrastructure for many organizations. In this electronically networked world, it is more important for organizations to manage various risks on IT components than to apply IT for competitive advantages [14]. As networked computers and connections to the Internet flourish, the numbers of unsecured and unpatched computers on the networks have also increased substantially in the recent past. These unsecured computers may result in serious threats to organizations and individuals alike. According to Computer Emergency Readiness Team (CERT), the number of computer security incidents has increased dramatically from 1996 to 2003 (Table 1).

For Internet based companies, threats to security or computer incidents can be serious problems which can affect business continuity. The CSI/FBI computer crime and security survey indicated that 95% of 700 organizations from both private and public sectors such as finance industry, high-tech industry, manufacturing, governments including federal, state and locals and educational institutions had experienced more than 10 website incidents during 2005. The incidents include denial of service, telecom fraud, unauthorized access to information, virus, financial fraud, insider abuse of net access, and system penetration [33]. The negative impact of security breaches has been discussed in several studies [15,36,40,41]. For companies, allocating resources to information security is imperative to keep their valuable information secure and to prevent damages stemming from IT vulnerabilities. According to the CIO survey, an average IT security budget in 2003 accounted for 11% of companies' IT budgets, up from 9.5% in 2002 [17].

A rational decision maker will invest further in information security if the cost of the investment is less than the risk of loss or if the investment itself has a positive return for the company. To accurately measure benefits and costs of information security investment, it is critical to have information about the likelihood of information security incidents as well as the impact of information security risks, which can be caused by unsecure information systems. However, one significant problem for companies in allocating resources for information security comes from the difficulty of measuring the cost and benefit of information security investment. Measuring the exact amount of return on information security investment (ROSI) is always challenging due to limited data for computing the likelihood and cost of information security risk factors. According to the report from the CISSP forum and the ISO27k implementer's forum, information security risk is defined as "a combination of the likelihood of an event, that are incidents or attacks on the information systems, cause negative impact on asset, group of asset or an organization" [18].

The report from the Government Accounting Office (GAO) points out the difficulties to assess information security risk. Since information security factors are continually changing because of rapidly developing technologies, it is very hard to acquire enough historical data to evaluate the likelihood and cost of information

* Corresponding author. Tel.: +82 2 940 4433.
E-mail address: mkkim@dongduk.ac.kr (M. Kim).

0167-9236/$ – see front matter © 2010 Elsevier B.V. All rights reserved.
doi:10.1016/j.dss.2010.08.017

Table 1
The number of security incidents reported to CERT.

Year	Number
1996	2573
1997	2134
1998	3734
1999	9859
2000	21,576
2001	52,658
2002	82,094
2003	137,529

security risk factors. The report also indicates that it is very complicated to try to estimate various indirect costs. For example, implementing new controls for securing information may lead to potential productivity loss in an organization, which is impossible to estimate [31].

While many studies in information system security focus on conceptual development [58] and economic models that suggest an optimal amount of security decision making and measurement [34,53], this study investigates the benefit of information security based on a firm's value in the stock market. Our study proposes that a firm's information security investment activity affects the market value of the firm. If there is a tangible impact on the value of a firm when security investment activities are disclosed, it can be interpreted as evidence for the value of the security investment to the firm.

Since the accurate measurement of benefits from information security investment is not easy, our study suggests another aspect of its benefits for the investment stakeholders by hypothesizing different stock market reactions accompanied by information security investment activities.

Based on an analysis of the relationship between information security investment announcements and the stock price change, this study finds empirical evidence for the economic value of information security investments.

We investigate the following research questions:

1. Do a firm's security investment announcements have a positive impact on its market value?
2. Does the stock market react differently to a firm's intention of investment in information security?
3. What is the effect of information security related laws on the market reaction to a firm's security investment activities?

To study these questions, we adopted an event methodology to observe investors' reactions to information security investment activities of firms. We tested our research hypotheses with public announcements of information security investment over a 10 year period from 1997 to 2006. Based on our results, we argue that our findings have significant implications for further research on the impact of information security investments and on the measurement of the economic value of information security investments.

2. Literature review

Prior research in the study of event methodology tradition in the area of management information systems can be classified into two: the literature that focuses on the *market impact of security breaches* [13,15,40,41] and the literature that focuses on *IT investment* [2,16,22,43].

The accurate estimation of security benefit is a key factor in performing the security economic analysis [8]. For effective security investment decision making, the benefit and cost estimation for a security investment is necessary. The cost of information security can be calculated by the capital or operating expenditure on hardware, software, and personnel [35]. Managers usually rely on data to support their decision making [4]. However, many security managers make a decision based on their experience, judgment, and their best knowledge because the benefit estimation for security investment has been difficult to determine due to a lack of historical data, a lack of effective metrics, and the complex and sensitive nature of security [12].

Several studies suggest using cost benefit analysis for effective information security decision making [12]; [29,35,45]. Effective security investment decisions can be made based on the analysis of expected loss from an information security risk and the benefits of information security investment which comes from the effectiveness of the countermeasure of security vulnerabilities and breaches as well as preventing future loss by mitigating information security risks. The research of Kim and Lee suggests a methodology can compute ROI of information security investment based on a cost and benefit factor analysis [45]. However, the largest body of information security research is mostly focused on the technical aspects of security such as the data encryption methods and access control [35].

Other researchers investigate the economic aspects of information security. Among the studies which use economic approaches to research information security, several use market reactions, based on abnormal returns, to calculate the direct cost of security risks [1,13,15,40,41,60].

The study of Campbell et al. [13] examines the economic effect of information security breaches reported in newspapers on publicly traded US corporations. They found that a highly significant negative market reaction to information security breaches involved unauthorized access to confidential data. In addition, they discovered differing stock market reactions depended on the degree of confidentiality of the breached data [13]. The research of Yayla and Hu investigates the impact of security breaches on stock value [64]. Hovav et al. also use market reactions to assess information security risk [40,41]. According to their research, the stock market has penalized Internet specific companies more frequently than non-Internet specific companies regarding denial-of-service attack announcements. For the breached firms in their sample set, an average 2.1% loss occurred in their market value within two days of the announcement. However, this security breach announcement positively affected the market value of security developers.

The study of Acquisiti et al. investigated how a company's privacy incidents affect its value in the market by examining stock price change [1]. Their findings indicated that an event of privacy breach has a significant negative influence on its stock price on the day when the privacy breach announcement was made. The economic implication of software vulnerability was also examined by event methodology. Telang and Wattal explored a stock market reaction to an announcement of software defects. They confirmed that a software defect announcement caused a significant loss of a firm's market value [60].

As we discussed previously, many studies have generated findings that the cost of poor security is very high so that a firm can face significant economic losses due to such information security incidents. The main purpose of this study is to examine the economic benefit of a firm's information security investment based on a firm's value on the stock market. Since there are several studies which focused on the economic benefits of information security investment by discussing how much such investment would increase returns [39,45,54], this study will contribute to the existing literature on the economic benefit of information security investment by suggesting a new approach to examine economic benefit of the investment.

3. Theoretical underpinnings and research hypotheses

Event methodology has been utilized in IT literature to examine the relationship between an IT event and its impact on a firm's value.