Abstract - As the collection of customers’ personal information is becoming economically feasible, security breaches are also increasing. Therefore, it is important to estimate the direct and indirect costs of personal information security breaches. In this study, we will examine the effects of personal information security breaches on the market values of breached firms and analyze the difference between IT and non-IT industries. This study will be formulated and conducted using the event study methodology. We aim to provide an investment standard of information security to corporate decision makers and calculate the costs of personal information breaches in the stock market.

Key-Words: - event study, security breaches, information security, privacy, personal information, customer information, security incidents

1 Introduction

Generally, through business transactions conducted on the Internet, companies’ collection of their customers’ personal information is steadily increasing. Personal information accumulated by firms has become a powerful business tool.

However, personal information does not only constitute a firm's asset but is also an individual’s private information. If personal information breaches occur, both individuals and firms are directly and indirectly affected. Nonetheless, Korean firms’ information security investment is low. According to a survey conducted by the Korea Communications Commission in 2012, Korean firms that invested in information security comprised 26.1 %, and 73.3% did not do so. Moreover, companies’ prevention activities for breaches decreased from the previous year. This survey shows that Korean firms have overlooked the importance of information security [11].

Studies have been conducted to measure the effects of security issues (such as security investments or information security breaches, etc.) on firms’ stock market values. However, related research in Korea has been done mostly in the early to mid-2000s. Korea has a more recent history of the stock market compared to those of other countries. Therefore, a study which can gather and analyze the most current events data is needed.

Based on relevant research, we have collected the latest data. Next, we will quantitatively measure the effects of personal information security breaches on firms’ market values by using the event study methodology. We will also analyze whether there is a significant difference between IT and non-IT industries. In this study, we expect to calculate the costs of personal information security breaches and to provide an investment standard of information security to decision makers of firms.

2 Related Research

2.1 Definition of IT Industry

This study aims to analyze the effects of personal information security breaches on firms’ market values.
values and whether there is a significant difference between IT and non-IT companies. Therefore, we first review the definitions of the IT and related industries (Table 1).

Table 1. Definitions of IT and related industries [1]

<table>
<thead>
<tr>
<th>Framework Act on Informatization Promotion</th>
<th>Information and communications are activities and measures to promote information collection, processing, storage, retrieval, transmission, reception, application, related equipment, related technology, related services and other informatization.</th>
</tr>
</thead>
</table>
| Special Purpose category of the National Statistical Office (information industry) | - Information and communication technology (ICT) industry  
  - Manufacturing industry: produces products by using electronic processing for the functions of processing, delivering or revealing information to control a physical process or to detect, measure and record a physical phenomenon  
  - Service industry: processes, transmits or reveals information by using electronic means  
  - Information content industry: produces and distributes information content to the general public  
  Information content is stored and sent in electronic media format. |
| OECD (Organisation for Economic Co-operation and Development) | - Information sector: "industries that support the electronic display, processing, storage and transmission of information"  
  - Content sector: The term "communication product" is used to describe the content that is displayed, processed, stored and transmitted electronically by the |

As shown in Table 1, the IT and related industries have been defined in various ways. Based on these definitions, events of the samples collected are classified under the IT and non-IT industries.

2.2 Occurrence of Personal Information Breaches

As previously stated, personal information collected by a firm is a firm’s asset, as well as the private information of individuals. If personal information breaches happen, they result in direct costs to companies and negative effects on the reliability of companies. Consequently, the issue may cause problems for future business activities.

Nevertheless, the scale of personal information breaches is becoming larger. According to the Korea Communications Commission, the number of breaches in personal information from 2011 to 2012 caused by hacking reached more than 60 million. Given 49 million population of Korea, Koreans experience leaks of personal information more than once per person [13].

Worldwide trends of personal information breaches scale also tend to larger. According to the Symantec Intelligence Report (August 2012 issue), the average incidence of data breaches in the world from January to August 2012 was 14 per month, which was lower than that from May to December 2011. Moreover, the number of disclosures of per-data breaches of personal information decreased by more than half; however, the median value of the same increased by 41% [12].

These statistical data showed that the physical number of data breaches decreased, but the number of disclosures of per-data breaches of personal information increased. This finding suggests that attackers capture specific information by employing targeted attacks.

2.3 Korean Studies on Effects of Information Security Issues on Firms’ Market Values

Nam (2006) studied the impacts of security events announcement on firms’ market values by using the event study methodology. In this study, security events were separated into security incidents and security failures.
Kim (2013) investigated the stock market reactions to newspaper reports of personal information security breaches that occurred in 2010–2012 in order to confirm the impact of the enforcement of the Privacy Act which protects personal information. She showed that personal information breaches affected firms’ market values. However, this study could not verify that investigation results were resulted in Privacy Act.

Kwon and Kim (2007) examined the association between information security investments and firms’ market values. At the same time, they studied the effects of information security breaches on firms’ market values. They showed that breached firms lost, on average, 0.86 % of their respective market values. In other words, the firms lost 54 billion won in market values. However, the authors could not find information on the security investments’ effects.

2.4 International Studies on Effects of Information Security Issues on Firms’ Market Values

Ettredge and Richardson (2001) examined the stock market reactions to the February 2000 denial-of-service attacks, and they analyzed the difference between non-Internet and Internet firms. They found that the attacks had negative effects on Internet firms more than they did on non-Internet firms.

Cavusglu, Mishara and Rahunathan (2004) investigated the effects of security breaches on capital markets by using the event study methodology. They analyzed the effects of firm type, firm size and year of the breach on the market reactions. They showed that breach cost was higher for Internet firms than those for conventional firms. Their study indicated that breached firms on the sample list lost, on average, 2.1 % of their respective market values within two days of the announcement. The average loss of breached firms was $1.65 billion in per breach in the capital market. However, the market value of security developers was different. The security developers on the sample list gained an average abnormal return of 1.36 % during the two-day period after the announcement. An average gain amounts to $1.06 billion in two days.

Acquisti, Friedman and Telang (2006) studied the effect of a company’s privacy breaches (which occurred in 2000–June 2006) on its market value. Their study showed a negative and statistically significant impact on the announcement day about the breach.

Masaki, Hideyuki, Kanta and Ichiro(2006) examined the economic effects of newspaper reports of information security incidents on firms’ values in the Japanese stock market. The sample comprised 70 companies over the 2002–August 2005 period. Their study showed that the response to newspaper reports of security incidents was slower in the Japanese stock market than in the US counterpart. There were significant reactions approximately 10 days after the newspaper reports. They also found that the price book-value ratio (PBR) and article size had substantial impacts on the firms’ market values.

3 Proposed Method

We will investigate the effects of personal information security breaches on firms’ market values by using the event study methodology. This method is used to assess the effect of a public announcement or a special event on the capital market. By using stock market returns as the basis of our proxy for economic effect, we will be able to capture both direct and indirect costs of the information security breaches [3].

3.1 Sample Selection

To date, we have collected news about breach events that occurred from January 2004 to August 2013 by conducting a keyword search in the Naver news online database. The reason why we chose Naver is that Naver is Korean largest portal site. We set up the first news day as the day of an event. The search keywords we have used are as follows:

Search Keywords : Personal information breaches, customer information leak, information disclosure, leak, private information, security incident, privacy information

We have not considered some of the search results which did not mention the breached firm’s name. Moreover, the news articles that reported events of multiple firms have been counted as multiple events. We chose events that reported at least 3 times. After the filtering process, we have been able to collect 62 breach events. In order to assess the difference in effect between firm types, we have classified our samples into IT and non-IT firms. The classification standards are based on previous research studies(Related Research 2.1), as follows:

- IT companies: computer companies, game companies, cell phone producers, portal
sites, wired and wireless network equipment manufacturers, software companies, semiconductor manufacturers, display manufacturers, telecom/network equipment and mobile communications sector

- Non IT companies: All other businesses except IT firms.

Table 2 presents basic statistics for the samples which we have collected until now.

Table 2. Basic Classification of Samples.

<table>
<thead>
<tr>
<th>Breached firm’s industry type</th>
<th>Number of samples</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT company</td>
<td>35</td>
</tr>
<tr>
<td>Non-IT company</td>
<td></td>
</tr>
<tr>
<td>Financial company</td>
<td>15</td>
</tr>
<tr>
<td>Non-financial company</td>
<td>13</td>
</tr>
</tbody>
</table>

As can be seen from Table 2, financial companies consist of a larger percentage of non-IT samples. Therefore, we will also investigate the difference between financial and non-financial companies.

3.2 Hypotheses
We have formulated the hypotheses based on previous research studies and our sample's characteristics. The hypotheses for the present study are the following:

H1: There is negative abnormal return when a personal information security breach is announced.

H2: The magnitude of the negative abnormal return will be larger when the breach of personal information happens with an IT firm than with a non-IT firm.

H3: The magnitude of the negative abnormal return will be larger when a financial company breaches personal information than when it is done by other non-IT firms.

3.3 Proposed Model
In this study, we will use the market model suggested by Eugene F. Fama (1995). To measure the effect of the news of personal information security breaches, we will estimate the normal returns by using the following linear model (1), with an estimation period of 250 days:

(1) \( R_{it} = \alpha_i + \beta_i \cdot R_{mt} + \epsilon_{it} \).

We will calculate the abnormal returns, which represent the deviations of realized returns from normal returns, as follows:

(2) \( AR_{it} = R_{it} - \alpha_i - \beta_i \cdot R_{mt} \).

4 Conclusion and Future Work
Relationships between firms’ market values and security issues have been studied to estimate the costs of security incidents and the benefits of security investments.

Previous research studies in Korea have shown that information security breaches affect the firms’ values in the Korean stock market. Therefore, in this study, we will investigate the effects of personal information security breaches and the difference between the IT and non-IT industries by using the event study methodology. We are currently monitoring and collecting additional data about personal information breach events which occurred from 2004 to August 2013. After the sample collection is completed, we will test the relationship between the two types of firms and verify our hypotheses. The purpose of this study is to provide an investment standard of information security for corporate decision makers and estimate the costs of personal information breaches in the stock market.

Acknowledgement
This research was supported by the MSIP(Ministry of Science, ICT & Future Planning), Korea, under the "Employment Contract based Master's Degree Program for Information Security" supervised by the KISA(Korea Internet Security Agency)(H2101-13-1001)

References:


