In Proceedings of the First Italian Conference on Cybersecurity (ITASEC17), Venice, Italy.

How does cyber crime affect firms? The effect of information security breaches on stock returns

Maria Cristina Arcuri[1], Marina Brogi[2] and Gino Gandolfi[1]

[1] Università degli Studi di Parma e SDA Bocconi School of Management
[2] Università di Roma "La Sapienza"

Abstract

A widely debated issue in recent years is cyber crime. Breaches in security of accessibility, integrity and confidentiality of information involve potentially high explicit and implicit costs for firms.

This paper investigates the impact of information security breaches on stock returns. Using event-study methodology, we provide empirical evidence on the effect of announcements of cyber attacks on the market value of firms from 1995 to 2015. We show that substantial negative market returns occur following announcements of cyber attacks. We find that financial entities often suffer greater negative effects than other companies. We also find that non-confidential cyber attacks are the most dangerous, especially for the financial sector. Our results seem to show a link between cyber crime and insider trading.

JEL Classification: G10; G15; G20
Keywords: cyber risk; cyber attack; information security; stock market

1. Introduction

The proliferation of information technology has affected all economic sectors, and although internet has often improved the way business is carried out, it has increased the vulnerability of critical infrastructures to information security breaches.

Cyber crime costs more than is often thought. It costs the global economy up to $450 billion every year, a figure higher than the market capitalization of Microsoft Inc. Furthermore, cyber attacks are becoming more frequent, more complex and bigger. Hamilton Place Strategies[1] reveals that in the last five years, the median cost of a cyber attack has increased by nearly 200 percent. From 2013 to 2015, cybercrime costs quadrupled and it appears that there will be another quadrupling from 2015 to 2019. Nevertheless, a significant portion of cybercrime goes undetected, e.g. industrial espionage gaining access to confidential information is difficult to spot.

Ginni Rometty, IBM Corp Chairman, CEO and President noted recently that cybercrime may be the greatest threat to every company in the world. Cyber risk represents, in fact, an enormous potential threat to public and private institutions because of its effects on organizational information systems, reputation, loss of stakeholders' confidence and financial losses. Sir

[1] Source: Hamilton Place Strategies (2015), *Cybercrime costs more than you think.*

Michael Rake, Chairman of BT Group, notes: "*Cyber Security matters to me because it fundamentally impacts the day to day activities of almost every individual and organisation. With technology positively influencing the flexibility, agility and global reach of our day to day business, it is vital that we seek to protect ourselves, our customers and our supply chain from the loss of personal or sensitive information. We also need to guard against the theft of intellectual property, damage to our reputation or brand and of course financial and commercial losses*".

Understanding the true impact of cyber attacks on stock market returns is crucial in deciding investment levels in information security activities. Cyber risk is thus a very important topic for all firms, including financial institutions. With reference to banks, Danièle Nouy, Chair of the Single Supervisory Mechanism (SSM) Supervisory Board, considers cyber risk as a risk related to data integrity, and notes that "*previously, banks dealt with the risk that IT system failures could hamper their daily operations, trigger operational losses and cause damage to their reputations. But in today's world, cyber risk also includes cyber attacks, the digital version of a classic bank robbery*". In light of this, in 2015, the SSM Supervisory Board performed a cyber security review and set up a process to closely monitor significant IT incidents at banks. The purpose was to gain an overview of trends and developments in cyber risk.

Several studies have examined the impact of announcements of cyber attack on the stock market returns of publicly traded companies. However, findings are mixed: the announcements have often, but not always, had a significant negative impact. Despite its importance, to our knowledge, there is currently little literature (Gordon and Loeb, 2002 and Anderson, 2001) on the economics of information security. Moreover, very little literature addresses the issue with reference to the financial sector. How large are negative market returns following cyber attacks? And do hackers use insider information for personal gain? The purpose of this paper is to empirically address these questions by analysing a large sample of firms between 1995 and 2015. We aim to understand whether negative market returns vary in size according to the sector (financial vs non-financial firms) and the nature of cyber attack.

The remainder of the paper proceeds as follows. In Section 2, we present a literature review. In Section 3 and 4, we describe the data and methodology. In Section 5, we discuss the results and in Section 6, we provide concluding comments.

2. Literature review

A large number of studies (Dos Santos et al. 1993; Oates 2001; Gordon and Loeb 2002; Garg et al. 2003; Gordon et al. 2003a; Ettredge and Richardson 2003; Hovav and D'Arcy 2003; Ko and Dorantes 2006; Andoh-Baidoo and Osei-Bryson 2007; Ishiguro et al. 2007; Kannan et al. 2007; Eisenstein 2008; Shackelford 2009; Winn and Govern 2009; Geers 2010; Kundur et al. 2011; Brockett et al. 2012; Odulaja and Wada 2012; Shackelford 2012) deal with information security breaches, but there is still a limited amount of literature related to the financial sector. The economic impact of cyber attacks is unclear. An information security breach can have negative economic impact, including lower sales revenues, higher expenses, decrease in future profits and dividends, worsening of reputation and reduction in the market value (Gordon et al. 2003b). However, the economic consequences can also be slight in the long run because firms can protect their main information assets, e.g. customer data or secret formulas. It is therefore possible that many information security breaches have insignificant economic impact. Some types of cyber attack are considered as a normal business cost for firms that use information technologies (Power 2002). Moreover, there is reason to believe that breached firms respond to cyber attacks by making new investment in information security (Campbell et al. 2003).

Market value represents the confidence that investors have in a firm, and measuring it is a way of calculating the impact of a cyber attack. Moreover, Bener (2000) states that investor behaviour depends on what they have observed in the past, i.e., investors take decisions in the light of the impact of security breaches on the market value of a firm in the past.

Several studies (Campbell et al. 2003; Cavusoglu et al. 2004; Hovav and D'Arcy 2004) use event study methodology to estimate the consequences of cyber attacks on the market value of breached firms. These studies also consider the type of breach. Campbell et al. (2003) state that the nature of the breach influences Cumulative Abnormal Return (CAR), while Cavusoglu et al. (2004) and Hovav and D'Arcy (2004) find that the nature of attack is not a determinant of CAR.

In general, there is a consensus that the announcement of a security breach leads to negative CAR. Campbell et al. (2003) focus on public firms and find a highly significant negative market reaction when breaches are related to unauthorized access to confidential data. Cavusoglu et al. (2004) find that breached firms lose average of 2.1% market value within 2 days of announcement. Acquisti et al. (2006) show that data breaches have a negative and statistically significant impact on a company's market value on the announcement day. Ishiguro et al. (2007) find statistically significant reactions in around 10 days after the news reports and observe that the reaction to news reports of the cyber attacks is slower on the Japanese stock market than on the US market. Gordon et al. (2011) conduct the analysis over two distinct sub-periods and find that the impact of information security breaches on stock market returns of firms is significant. In particular, attacks associated with breaches of availability are seen to have the greatest negative effect on stock market returns. Some studies (Cohen 1997a; Cohen 1997b; Cohen et al. 1998) present a list of sets of attacks, defences and effects. The attacker's motivations can also determine the level of attack intensity (Gupta et al. 2000).

To our knowledge, there is little literature on the economics of information security. Gordon and Loeb (2002) present an economic model that determines the optimal amount to invest to protect a given set of information. They suggest that to maximize the expected benefit from investment in protecting information, a firm should spend only a small fraction of the expected loss caused by a security breach. Anderson (2001) puts forward a new concept of information insecurity, based on factors including network externalities, asymmetric information, moral hazard and adverse selection. Kahn and Roberds (2008) focus on identity theft in credit transactions, which they call "the quintessential crime of the information age", and model a trade-off between a desire to avoid costly/invasive monitoring of individuals and the need to control economic transactions. Cashell et al. (2004) point out the importance of information security in both public and private sectors. They focus on the resources used for information security, and find that economic analysis can supply important information.

Overall, the number of studies dealing with information security breaches in the financial industry is limited. The main contribution of our paper is that it focuses on a longer period, 1995-2015, and presents a comparison between the financial and other sectors. Information security is a very important issue in the financial sector, especially in the light of its potential impact on reputation. For financial intermediaries reputation is, in fact, crucial, considering that the supply of payment, risk management services and asymmetric information all create systemic risk (Bhattachrya and Thakor 1993; Allen and Santomero 1997, 2001). And given that today the banking industry has significant online presence (Pennathur 2001), cyber risk is an important category of banking risk. The second contribution to the literature is that our study considers the 'nature' of information security breaches in terms of whether they are confidential or non-confidential. This difference appears to be a determinant of whether and why a cyber attack is likely to be a costly burden for a firm and its shareholders.

3. Data

We selected our sample from the Factiva database, searching for newspaper reports of cyber attacks 1995-2015[2]. We used the following key words: "information security breach", "cyber attack", "computer break-in", "computer attack", "computer virus", "computer system security", "bank computer attack", "internet security incident", "denial of service attack", "hacker".

We initially identified 252 information security breaches (i.e., events). We obtained stock market prices from the Datastream database, which were adjusted for dividends and splits. To be included in our sample, information on the stock prices of the firms had to be available in this database. So our final sample includes 226 cyber attacks affecting 110 firms. Of these 226 security breaches, 67 affected 34 financial entities.

Table 1 reports the industry distribution of the sample of cyber attacks. Companies belonging to following sectors, Software Publishers, Electronic Shopping and All Other Telecommunications, announced the highest number of cyber attacks; 37, 15 and 12 respectively. The Finance and Insurance sector announced 67 cyber attacks (see Appendix).

Table 2 shows event distribution over the period 1995-2015. In the three years (2013-2015), the sample companies suffered from almost 30% of total cyber attacks. In particular, financial companies registered over 41% and non-financial companies registered about 25% of cyber attacks. Cyber security is thus becoming an increasingly important issue.

Table 1: Sample industry distribution of the final sample

NAICS	Industry description	No. of firms
221118	Other Electric Power Generation	1
312111	Soft Drink Manufacturing	1
316211	Rubber and Plastics Footwear Manufacturing	1
324110	Petroleum Refineries	1
325412	Pharmaceutical Preparation Manufacturing	2
325620	Toilet Preparation Manufacturing	1
332312	Fabricated Structural Metal Manufacturing	1
333315	Photographic and Photocopying Equipment Manufacturing	1
334111	Electronic Computer Manufacturing	3
334112	Computer Storage Device Manufacturing	1
334119	Other Computer Peripheral Equipment Manufacturing	1
334210	Telephone Apparatus Manufacturing	2
336411	Aircraft Manufacturing	2
336414	Guided Missile and Space Vehicle Manufacturing	1
441228	Motorcycle, ATV, and All Other Motor Vehicle Dealers	3
441229	All Other Motor Vehicle Dealers	2

[2] In line with previous literature, we chose 1995 as the beginning date because it coincides with the emergence of the Internet.

443120	Computer & Software Stores	1
443142	Electronics Stores	2
445110	Supermarket and Other Grocery (Except Convenience) Stores	1
446110	Pharmacies & Drug Stores	1
448140	Family Clothing Stores	2
451120	Hobby, Toy, & Game Stores	1
451211	Book Stores	1
452990	All Other General Merchandise Stores	1
453210	Office Supplies and Stationery Stores	1
454111	Electronic Shopping	5
481111	Scheduled Passenger Air Transportation	3
482111	Line-Haul Railroads	1
492110	Couriers	2
511110	Newspaper Publishers	3
511210	Software Publishers	5
513322	Cellular and Other Wireless Telecommunications	2
515210	Cable and Other Subscription Programming	1
517110	Wired Telecommunications Carriers	2
517210	Wireless Telecommunications Carriers	1
517919	All Other Telecommunications	4
518210	Data Processing & Related Services	3
519130	Internet Publishing and Broadcasting and Web Search Portals	1
520000	Finance and Insurance	34
541410	Interior Design Services	2
541511	Custom Computer Programming Services	2
541519	Other computer related services	1
561311	Employment Placement Agencies	1
561621	Security Systems Services (except Locksmiths)	1
811213	Communication Equipment Repair and Maintenance	1
Total		**110**

Notes: The table shows the sample industry distribution of the final sample following the North American Industry Classification System (NAICS).

Table 2: Event distribution of the final sample 1995-2015

	Total sample		**Financial entities**		**Non-Financial companies**	
Year	**No of events**	**% of the sample**	**No of events**	**% of the sample**	**No of events**	**% of the sample**
1995	2	0.88%	1	1.49%	1	0.63%
1996	1	0.44%	0	0.00%	1	0.63%
1997	4	1.77%	0	0.00%	4	2.52%
1998	2	0.88%	0	0.00%	2	1.26%

1999	17	7.52%	3	4.48%	14	8.81%
2000	22	9.73%	2	2.99%	20	12.58%
2001	11	4.87%	3	4.48%	8	5.03%
2002	4	1.77%	0	0.00%	4	2.52%
2003	10	4.42%	3	4.48%	7	4.40%
2004	10	4.42%	2	2.99%	8	5.03%
2005	11	4.87%	5	7.46%	6	3.77%
2006	3	1.33%	2	2.99%	1	0.63%
2007	10	4.42%	3	4.48%	7	4.40%
2008	3	1.33%	0	0.00%	3	1.89%
2009	10	4.42%	3	4.48%	7	4.40%
2010	11	4.87%	2	2.99%	9	5.66%
2011	13	5.75%	1	1.49%	12	7.55%
2012	15	6.64%	9	13.43%	6	3.77%
2013	31	13.72%	15	22.39%	16	10.06%
2014	17	7.52%	3	4.48%	14	8.81%
2015	19	8.41%	10	14.93%	9	5.66%
Total	**226**		**67**		**159**	

Notes: The table shows cyber attack distribution of the final sample from 1995 to 2015.

4. Methodology

Following previous studies (Campbell et al. 2003; Gordon et al. 2011), we run an event study to measure the impact of information security breaches on stock returns. This methodology makes it possible to verify whether cyber criminals are involved in insider trading. Event study methodology has been widely used in banking and finance literature (see, e.g., Brown and Warner 1980). The assumption is that the financial markets respond to news affecting the value of a security, so stock market returns are able to capture the implicit and explicit costs of cyber attacks (Acquisti et al. 2006; Iheagwara et al. 2004; Kerschbaum et al. 2002; McConnell and Muscarella 1985). In particular, if a firm suffers from an information security breach then it may incur financial losses, which should reflect in its stock price. Stock prices on the days surrounding the event can capture the impact of that event and measure the economic cost of the cyber attack. Event study methodology is in fact based on a semi-strong version of the efficient market hypothesis (Fama et al. 1969).

First, we calculate abnormal returns (ARs), or forecast errors of a specific normal return-generating mode. Estimated ARs are defined as the company stock return obtained on a given day *t*, i.e. when the cyber attack is announced, minus the predicted "normal" stock return. We estimate daily AR using the Sharpe (1963) market model as follows:

$$R_{i,t} = \alpha_i + \beta_i R_{m,t} + \varepsilon_{i,t} \tag{1}$$

where $R_{i,t}$ is the stock rate of return of the affected company *i* on day *t*; $R_{m,t}$ is the rate of return on market index on day *t*; α_i is the idiosyncratic risk component of share *i*; β_i is the beta coefficient of share *i* and εi,t is the random error. The αi and βi coefficients were estimated for each company using an ordinary least square (OLS) regression of Ri,t on Rm,t for a 121-working-day estimation period (from the 21st to the 141th day before the cyber attack announcement). The event window is defined as the time window that takes into account -τ1 days before and +τ2 day after the date of the announcement. The date of the announcement is defined as day zero. Following a standard approach, we consider various event windows with different lengths, with the widest lasting from 20 days before the announcement day to 20 days after it. Because our sample includes a large set of firms, we select the following market indexes: the S&P500 Composite[3], NASDAQ and the S&P600 Small Cap. We use the market index total return as our proxy of Rm,t[4]. Using the firm-specific parameters estimated for the market model over the estimated period, the ARi,t is measured as follows:

$$AR_{i,t} = R_{i,t} - (\alpha_i + \beta_i R_{m,t}) \tag{2}$$

The average AR for *n* firm shares on day *t* ($\overline{AR_t}$) of the event window is measured as follows:

$$\overline{AR_t} = \frac{1}{n} \sum_{i=1}^{n} AR_{i,t} \tag{3}$$

We compute the cumulative abnormal return (CARi) over the event window as follows:

$$CAR_i\,(\tau 1, \tau 2) = \sum_{t=\tau 1}^{\tau 2} AR_{i,t} \tag{4}$$

where the (τ1, τ2) is the event window.

The average CAR for the event period [$\overline{CAR}$ (τ1, τ2)] is measured as follows:

$$\overline{CAR\,(\tau 1, \tau 2)} = \frac{1}{n} \sum_{i=1}^{n} CAR_i\,(\tau 1, \tau 2) \tag{5}$$

where *n* is the number of events.

We test the statistical significance of CARs using the Boehmer et al. (1991) test statistic Z to capture the event-induced increase in return volatility as follows:

$$Z = \sqrt{n}\, \frac{\overline{SCAR}\,(\tau 1, \tau 2)}{\sqrt{((1/(n-1)) \sum (SCAR\,(\tau 1, \tau 2) - \overline{SCAR}\,(\tau 1, \tau 2))^2}} \approx T\,(0, g/\,g\text{-}2) \tag{6}$$

[3] Subramani and Walden (2001) use the S&P 500 Composite index.

[4] Some studies use a set of control firms in the same industry to assess AR, e.g., Cooper et al. (2001).

where *n* is the number of the stocks in the sample and SCAR $(-\tau 1, \tau 2)$ is the standardized abnormal return on stocks *i* at day t, obtained following the Mikkelson and Partch (1988) approach as follows:

$$SCAR_{i,t} = \frac{CAR_{i}\,(\tau 1, \tau 2)}{\sigma_i \sqrt{T_s + T_s^2/T} + \sum_{i=\tau 1}^{\tau 2} (R_{m,t} - T_s \overline{R}_m) / \sum_{i=1}^{T} (R_{m,t} - \overline{R}_m)} \tag{7}$$

where Rm is the average return on market index in the estimation period, σi is the estimated standard deviation of AR on stock *i*, T is the number of days in the estimation period, Ts is the number of days in the event window and all other terms as previously defined. The Z test in Equation (6) has a t-distribution with T-2 degrees of freedom and converges to a unit normal. We also carried out the following two tests. The first, described by Campbell et al. (1997), verifies whereby the event has no influence on CARs (null hypothesis) as follows:

$$T_1 = \frac{CAR\,(\tau 1, \tau 2)}{\sqrt{\sigma^2(\tau 1, \tau 2)}} \approx N(0,1) \tag{8}$$

The second, called the Sign test (Peterson, 1989; Campbell et al. 1997; MacKinlay, 1997), is a non-parametric test used to validate the results of the test Z and T_1, as follows:

$$T_2 = \left[\frac{N^{(-)}}{N} - 0{,}5 \right] \frac{N^{1/2}}{0{,}5} \approx N(0,1) \tag{9}$$

where N is the number of events and $N^{(-)}$ is the number of event with negative CAR. The null hypothesis is represented by the absence of significant CARs in the presence of announcements of cyber attacks. The key parameter of the T_2 is the median sample and the null hypothesis is rejected when a significant number of negative CARs are recorded.

5. Results

Focusing on the whole sample of cyber attacks (Table 3), we found that the average CARs are negative in all event windows, showing that cyber attack announcements always lead to negative market returns for a company. The extent of negative market returns and the statistical significance of mean CARs vary according to the event windows. In particular, results in the symmetric event windows after the announcement show a high statistical significance, at the 90% confidence level or above. The event windows (-5; 5) and (-3; 3) show mean CARs of -1.26% and -1.19% respectively. This means that significant negative market returns occur on the days prior to and after the announcement of information security breaches. Moreover, the official announcement of a cyber attack is often partly anticipated by a few days: the asymmetric event windows (-10; -1), (-5; -1) and (-3; -1) display a statistical significance at the 90% confidence level or above. Specifically, they show mean CARs of -1.08%, -0.87% and -0.90% respectively. These results imply that cyber criminals are in fact implicated in insider trading. Finally, negative market returns also occur on the days after the announcement: the event window (0; 20) shows a mean CAR of -1.19%, but at low statistical significance.

Table 3: Test statistics on CARs for the whole sample

Event window	No. of observations	Mean CAR (%)	Z	T_1	T_2	% of negative CARs
(-20; 20)	226	-3.326	-1.361*	-1.634*	-0.399	48.67
(-10; 10)	226	-3.334	-2.360***	-2.190***	0.399	51.33
(-5; 5)	226	-1.257	-2.389***	-2.818***	2.794***	59.29
(-3; 3)	226	-1.190	-2.313***	-2.987***	2.129***	57.08
(-20; -1)	226	-0.991	-1.667*	-1.341*	0.532	51.77
(-10; -1)	226	-1.083	-2.681***	-2.479***	2.395***	57.96
(-5; -1)	226	-0.874	-3.820***	-2.971***	4.257***	64.16
(-3; -1)	226	-0.900	-3.429***	-3.718***	3.991***	63.27
(0; 20)	226	-1.194	-1.841**	-1.599*	0.931	53.10
(0; 10)	226	-2.251	-0.970	-1.754**	-0.266	49.12
(0; 5)	226	-0.382	0.183	-1.041	-0.133	49.56
(0; 3)	226	-0.290	-0.143	-0.885	-0.798	47.35
(0; 1)	226	-0.238	0.357	-0.855	-2.661	41.15

Notes: The table reports the results of the event study carried out on the data for 226 cases of cyber attacks announced by 110 listed companies between 1995 and 2015. We measured the companies' normal return as reported in Equation (1). The abnormal return (Ari,t) was calculated as reported in Equation (2). The CAR statistical significance was assessed using the parametric tests Z and T_1 reported in Equations (6) and (8) and the non-parametric test T_2 reported in Equation (9).
* Statistically significant at 10% (one-tailed test)
** Statistically significant at 5% (one-tailed test)
*** Statistically significant at 1% (one-tailed test)

We classify the sample according to the economic sector of the firms. In particular, we analyse the potential differences between the financial sand other sectors. Tables 4 and 5 report the results. We found that the average CARs are negative in all event windows, showing that cyber attack announcements lead to negative market returns for both financial and non-financial companies. Moreover, the official announcement of information security breach is partly anticipated by a few days. With reference to the financial sector, the event windows (-10; -1), (-5; -1) and (-3; -1) display a high statistical significance and show mean CARs of -2.04%, -0.91% and -0.80% respectively. For the other sectors, the event windows (-10; -1), (-5; -1) and (-3; -1) display a high statistical significance and show mean CARs of -0.68%, -0.86% and -0.94% respectively. Again, it seems that a link exists between cyber crime and insider trading. The other sectors also register statistical significant mean CARs in the event windows (-5; 5) and (-3; 3), - 1.18% and -1.22% respectively.

In general, financial entities show a greater negative effect in the event windows before the cyber attack announcements.

Table 4: Test statistics on CARs for financial entities

Event window	No. of observations	Mean CAR (%)	Z	T_1	T_2	% of negative CARs
(-20; 20)	67	-3.423	-1.389*	-2.544***	0.122	50.75
(-10; 10)	67	-3.107	-2.323***	-3.373***	1.100	56.72
(-5; 5)	67	-1.446	-1.640*	-2.700***	1.100	56.72
(-3; 3)	67	-1.121	-1.730**	-2.648***	1.100	56.72

(-20; -1)	67	-2.111	-0.841	-2.418***	0.367	52.24
(-10; -1)	67	-2.041	-2.582***	-3.435***	2.321***	64.18
(-5; -1)	67	-0.910	-1.477*	-2.743***	2.321***	64.18
(-3; -1)	67	-0.797	-1.726**	-3.310***	2.077***	62.69
(0; 20)	67	-2.154	-0.764	-2.276***	0.855	55.22
(0; 10)	67	-1.067	-0.925	-1.752**	0.611	53.73
(0; 5)	67	-0.536	-0.248	-1.291*	0.122	50.75
(0; 3)	67	-0.324	0.014	-0.790	-0.122	49.25
(0; 1)	67	-0.165	0.737	-0.441	-0.367	47.76

Notes: The table reports the results of the event study carried out on the data for 67 cases of cyber attacks announced by 34 listed financial companies between 1995 and 2015. We measured the companies' normal return as reported in Equation (1). The abnormal return (Ari,t) was calculated as reported in Equation (2). The CAR statistical significance was assessed using the parametric tests Z and T_1 reported in Equations (6) and (8) and the non-parametric test T_2 reported in Equation (9).

* Statistically significant at 10% (one-tailed test)

** Statistically significant at 5% (one-tailed test)

*** Statistically significant at 1% (one-tailed test

Table 5: Test statistics on CARs for non-financial entities

Event window	No. of observations	Mean CAR (%)	Z	T_1	T_2	% of negative CARs
(-20; 20)	159	-3.284	-0.687	-1.158	-0.872	46.54
(-10; 10)	159	-3.430	-1.326*	-1.611*	0.079	50.31
(-5; 5)	159	-1.177	-1.826**	-1.987**	2.776***	61.01
(-3; 3)	159	-1.219	-1.723**	-2.268***	1.824**	57.23
(-20; -1)	159	-0.520	-1.442*	-0.529	0.555	52.20
(-10; -1)	159	-0.679	-2.058***	-1.202*	1.348*	55.35
(-5; -1)	159	-0.859	-3.537***	-2.179***	3.410***	63.52
(-3; -1)	159	-0.943	-3.051***	-2.869***	3.727***	64.78
(0; 20)	159	-0.790	-1.705**	-0.804	0.714	52.83
(0; 10)	159	-2.750	-0.565	-1.524*	-0.714	47.17
(0; 5)	159	-0.317	0.315	-0.646	0.079	50.31
(0; 3)	159	-0.276	-0.183	-0.637	-0.714	47.17
(0; 1)	159	-0.268	-1.624	-0.741	-0.714	47.17

Notes: The table reports the results of the event study carried out on the data for 159 cases of cyber attacks announced by 76 listed financial companies between 1995 and 2015. We measured the companies' normal return as reported in Equation (1). The abnormal return (Ari,t) was calculated as reported in Equation (2). The CAR statistical significance was assessed using the parametric tests Z and T_1 reported in Equations (6) and (8) and the non-parametric test T_2 reported in Equation (9).

* Statistically significant at 10% (one-tailed test)

** Statistically significant at 5% (one-tailed test)

*** Statistically significant at 1% (one-tailed test

Next, we present our results by grouping information security breaches according to whether the attack is confidential (75 events) or non-confidential (151 events). We consider a cyber attack as confidential where unauthorized access to confidential information occurs, and non-confidential when it is a computer virus or worm, a DOS attack or system breakdown.

First, we analyse the whole sample. Regarding confidential attacks (Table 6), we found that all mean CARs are negative [except for the event windows (-5; 5), (0; 5) and (0; 3)] but their size is generally small and they are not statistically significant (i.e. they are below the 90% confidence level), except for the event windows (-10; -1) and (-5; -1). The event window (-10; -1) shows mean CARs of -0.17% but it is not completely reliable because the result passes only the parametric Z test. The event window (-5; -1) shows mean CARs of -0.18%. Regarding non-confidential attacks (Table 7), we found that all mean CARs are negative and higher in symmetric event windows, ranging from -1.68% to -4.71%, and with a confidence level of 90% or more. The event windows (-10; -1), (-5; -1) and (-3; -1) also display a high statistical significance and show mean CARs of -1.53%, -1.22% and -1.18% respectively. This means that investors are able to forecast non-confidential cyber attacks.

Table 6: Test statistics on CARs for sub-sample of confidential attacks for the whole sample

Event window	No. of observations	Mean CAR (%)	Z	T_1	T_2	% of negative CARs
(-20; 20)	75	-0.153	0.330	-0.084	-1.270	42.67
(-10; 10)	75	-0.565	-0.010	-0.396	-1.039	44.00
(-5; 5)	75	0.040	-0.241	0.065	0.577	53.33
(-3; 3)	75	-0.210	0.039	-0.398	0.115	50.67
(-20; -1)	75	-0.552	-1.015	-0.729	-0.346	48.00
(-10; -1)	75	-0.173	-1.364*	-0.262	1.039	56.00
(-5; -1)	75	-0.183	-1.348*	-0.479	1.963**	61.33
(-3; -1)	75	-0.327	-0.922	-1.195	1.501**	58.67
(0; 20)	75	-0.743	-1.027	-0.924	0.115	50.67
(0; 10)	75	-0.391	0.872	-0.315	-1.039	50.67
(0; 5)	75	0.223	0.693	0.413	-1.039	44.00
(0; 3)	75	0.116	0.864	0.240	-1.501	44.00
(0; 1)	75	-0.058	0.751	-0.137	-2.194***	37.33

Notes: The table reports the results of the event study carried out on the data for 75 cases of confidential cyber attacks announced by 51 listed companies between 1995 and 2015. We measured the companies' normal return as reported in Equation (1). The abnormal return (Ari,t) was calculated as reported in Equation (2). The CAR statistical significance was assessed using the parametric tests Z and T_1 reported in Equations (6) and (8) and the non-parametric test T_2 reported in Equation (9).

* Statistically significant at 10% (one-tailed test)

** Statistically significant at 5% (one-tailed test)

*** Statistically significant at 1% (one-tailed test)

Table 7: Test statistics on CARs for sub-sample of non-confidential attacks for the whole sample

Event window	No. of observations	Mean CAR (%)	Z	T_1	T_2	% of negative CARs
(-20; 20)	151	-4.901	-1.809**	-1.691*	0.407	51.66
(-10; 10)	151	-4.710	-2.839***	-2.183***	1.546*	56.29
(-5; 5)	151	-1.901	-2.699***	-3.248***	3.174***	62.91
(-3; 3)	151	-1.676	-2.928***	-3.158***	2.523***	60.26
(-20; -1)	151	-1.210	-1.328*	-1.163	0.895	53.64
(-10; -1)	151	-1.535	-2.384***	-2.735***	2.360***	59.60
(-5; -1)	151	-1.218	-3.619***	-3.087***	3.988***	66.23
(-3; -1)	151	-1.184	-3.355***	-3.552***	4.313***	67.55
(0; 20)	151	-1.419	-1.528*	-1.359*	1.383*	55.63
(0; 10)	151	-3.175	-1.747**	-1.750**	0.407	51.66
(0; 5)	151	-0.683	-0.227	-1.430*	0.895	53.64
(0; 3)	151	-0.492	-0.641	-1.153	0.244	50.99
(0; 1)	151	-0.327	-1.033	-0.911	0.570	52.32

Notes: The table reports the results of the event study carried out on the data for 151 cases of non-confidential cyber attacks announced by 86 listed companies between 1995 and 2015. We measured the companies' normal

return as reported in Equation (1). The abnormal return (Ari,t) was calculated as reported in Equation (2). The CAR statistical significance was assessed using the parametric tests Z and T_1 reported in Equations (6) and (8) and the non-parametric test T_2 reported in Equation (9).
* Statistically significant at 10% (one-tailed test)
** Statistically significant at 5% (one-tailed test)
*** Statistically significant at 1% (one-tailed test)

We also measured the effects on market returns of confidential and non-confidential attacks distinguishing between financial entities and non-financial companies. In the case of confidential attacks announced by financial entities (Table 8), we found no statistically significant results. In the financial industry, confidential attack announcements are likely to be predicted by investors because unauthorized access to confidential information is a big concern, and word of mouth is likely to spread fast.

Non-confidential attacks announced by financial entities (Table 9) appear to generate greater negative market returns than confidential attacks. The most significant results were found in the symmetric event windows (-10; 10), (-5; 5) and (-3; 3), showing statistically significant CARs of -4.03%, -1.92% and -1.46%, respectively. Statistical significant negative market returns are also associated with the event windows (-10; -1), (-5; -1) and (-3; -1), with values of -2.63%, -1.34% and -1,00%, respectively.

Interestingly, non-confidential attacks in the financial system are more dangerous than confidential attacks. This may signal that the stock markets are more efficient when cyber attacks do not concern access to confidential information. In general, non-confidential attacks determine larger negative returns than the confidential ones, so it may be the case that investors perceive financial entities damaged by non-confidential attacks as being more vulnerable. In fact, as well as protecting data, such as customer records, trading information, and confidential documents, banks and other financial service organizations have to safeguard their systems and networks as well as their financial assets. This means the financial sector faces a larger number of threats than many other industries.

Table 8: Test statistics on CARs for sub-sample of confidential attacks for financial entities

	No. of	Mean CAR				% of negative
Event window	observations	(%)	Z	T_1	T_2	CARs
(-20; 20)	23	-1.232	-0.067	-0.652	-0.209	47.83
(-10; 10)	23	-1.338	-0.752	-0.974	-0.209	47.83
(-5; 5)	23	-0.540	0.129	-0.718	-0.209	47.83
(-3; 3)	23	-0.465	0.332	-0.554	-0.626	43.48
(-20; -1)	23	-1.116	0.050	-0.773	-0.209	47.83
(-10; -1)	23	-0.922	-0.079	-0.984	0.626	56.52
(-5; -1)	23	-0.090	0.529	-0.199	0.209	52.17
(-3; -1)	23	-0.407	-0.010	-0.876	-0.209	47.83
(0; 20)	23	-1.309	0.117	-0.801	0.209	52.17
(0; 10)	23	-0.416	-0.361	-0.528	-0.209	47.83
(0; 5)	23	-0.450	0.009	-0.082	-0.209	47.83
(0; 3)	23	-0.058	0.958	-0.082	-0.626	43.48
(0; 1)	23	-0.326	1.026	-0.483	-1.043	39.13

Notes: The table reports the results of the event study carried out on the data for 23 cases of confidential cyber attacks announced by 15 listed financial companies between 1995 and 2015. We measured the companies' normal return as reported in Equation (1). The abnormal return (Ari,t) was calculated as reported in Equation (2). The CAR statistical significance was assessed using the parametric tests Z and T_1 reported in Equations (6) and (8) and the non-parametric test T_2 reported in Equation (9).
* Statistically significant at 10% (one-tailed test)
** Statistically significant at 5% (one-tailed test)

*** Statistically significant at 1% (one-tailed test

Table 9: Test statistics on CARs for sub-sample of non-confidential attacks for financial entities

Event window	No. of observations	Mean CAR (%)	Z	T_1	T_2	% of negative CARs
(-20; 20)	44	-4.569	-1.539*	-2.579***	0.905	56.82
(-10; 10)	44	-4.032	-2.250***	-3.412***	1.508*	61.36
(-5; 5)	44	-1.920	-1.978**	-2.727***	1.508*	61.36
(-3; 3)	44	-1.464	-2.392***	-3.153***	1.809**	63.64
(-20; -1)	44	-2.631	-1.042	-2.422***	0.603	54.55
(-10; -1)	44	-2.626	-3.114***	-3.522***	2.714***	70.45
(-5; -1)	44	-1.339	-2.583***	-3.091***	2.714***	70.45
(-3; -1)	44	-1.001	-1.847**	-3.710***	2.714***	70.45
(0; 20)	44	-2.596	-0.968	-2.248***	0.905	56.82
(0; 10)	44	-1.407	-0.856	-1.703**	0.905	56.82
(0; 5)	44	-0.581	-0.285	-1.102	0.302	52.27
(0; 3)	44	-0.462	-0.418	-0.922	0.302	52.27
(0; 1)	44	-0.081	-0.625	-0.180	0.302	52.27

Notes: The table reports the results of the event study carried out on the data for 44 cases of non-confidential cyber attacks announced by 26 listed financial companies between 1995 and 2015. We measured the companies' normal return as reported in Equation (1). The abnormal return (Ari,t) was calculated as reported in Equation (2). The CAR statistical significance was assessed using the parametric tests Z and T_1 reported in Equations (6) and (8) and the non-parametric test T_2 reported in Equation (9).
* Statistically significant at 10% (one-tailed test)
** Statistically significant at 5% (one-tailed test)
*** Statistically significant at 1% (one-tailed test

Focusing on confidential attacks announced by non-financial companies (Table 10), we found no statistically significant results except for the event window (-5; -1). Again, we found that confidential attack announcements are likely to be forecast by investors. Regarding non-confidential attacks announced by non-financial companies (Table 11), CARs are negative and statistically significant at -1.89% and -1.76% for the event windows (-5; 5) and (-3; 3), respectively. Statistically significant negative market returns are also associated with the event windows (-5; -1) and (-3; -1), with values of -1.17%, and -1.26%, respectively.

Finally, we found that non-confidential attacks are more dangerous than confidential attacks for both financial and non-financial sectors but, in general, the negative effects on the financial sector are greater than on other sectors. Most mean CARs values are statistically significant and higher than values in other sectors.

Table 10: Test statistics on CARs for sub-sample of confidential attacks for other sectors

Event window	No. of observations	Mean CAR (%)	Z	T_1	T_2	% of negative CARs
(-20; 20)	52	0.324	0.422	0.130	-1.387*	40.38
(-10; 10)	52	-0.223	0.377	-0.113	-1.109	42.31
(-5; 5)	52	0.297	-0.329	0.360	0.832	55.77
(-3; 3)	52	-0.098	-0.112	-0.147	0.555	53.85
(-20; -1)	52	-0.302	-1.254*	-0.342	-0.277	48.08
(-10; -1)	52	0.158	-1.518*	0.184	0.832	55.77
(-5; -1)	52	-0.224	-2.102***	-0.436	2.219***	65.38
(-3; -1)	52	-0.291	-1.111	-0.866	0.832	63.46

(0; 20)	52	-0.493	-1.297*	-0.545	0.000	50.00
(0; 10)	52	-0.380	1.174	-0.217	-1.109	42.31
(0; 5)	52	0.521	0.740	0.727	-1.109	42.31
(0; 3)	52	0.193	0.462	0.309	-1.387*	40.38
(0; 1)	52	0.061	-1.041	0.115	-1.941**	36.54

Notes: The table reports the results of the event study carried out on the data for 52 cases of confidential cyber attacks announced by 36 listed companies between 1995 and 2015. We measured the companies' normal return as reported in Equation (1). The abnormal return (Ari,t) was calculated as reported in Equation (2). The CAR statistical significance was assessed using the parametric tests Z and T_1 reported in Equations (6) and (8) and the non-parametric test T_2 reported in Equation (9).
* Statistically significant at 10% (one-tailed test)
** Statistically significant at 5% (one-tailed test)
*** Statistically significant at 1% (one-tailed test

Table 11: Test statistics on CARs for sub-sample of non-confidential attacks for other sectors

Event window	No. of observations	Mean CAR (%)	Z	T_1	T_2	% of negative CARs
(-20; 20)	107	-5.038	-1.111	-1.252*	-0.097	49.53
(-10; 10)	107	-4.988	-1.907**	-1.660**	0.870	54.21
(-5; 5)	107	-1.893	-1.982**	-2.447***	2.804***	63.55
(-3; 3)	107	-1.764	-2.080***	-2.435***	1.837***	58.88
(-20; -1)	107	-0.626	-0.908	-0.449	0.870	54.21
(-10; -1)	107	-1.086	-1.706**	-1.497*	0.870	54.21
(-5; -1)	107	-1.168	-2.958***	-2.214***	2.997***	64.49
(-3; -1)	107	-1.260	-2.862***	-2.756***	3.384***	66.36
(0; 20)	107	-0.935	-1.189	-0.672	1.063	55.14
(0; 10)	107	-3.902	-1.532**	-1.539**	-0.097	49.53
(0; 5)	107	-0.725	-0.113	-1.136	0.870	54.21
(0; 3)	107	-0.504	-0.489	-0.891	-0.097	49.53
(0; 1)	107	-0,428	-1.942**	-0.908	0.483	52.34

Notes: The table reports the results of the event study carried out on the data for 107 cases of non-confidential cyber attacks announced by 58 listed companies between 1995 and 2015. We measured the companies' normal return as reported in Equation (1). The abnormal return (Ari,t) was calculated as reported in Equation (2). The CAR statistical significance was assessed using the parametric tests Z and T_1 reported in Equations (6) and (8) and the non-parametric test T_2 reported in Equation (9).
* Statistically significant at 10% (one-tailed test)
** Statistically significant at 5% (one-tailed test)
*** Statistically significant at 1% (one-tailed test

6. Conclusions

Internet is an important driver of economic development, but dependence on cyberspace has increased the vulnerability of critical infrastructures to information security breaches. Market value represents the confidence that investors have in a firm, and measuring make it possible to calculate the impact of a cyber attack.

In this paper, we study the effects on market returns of the announcement of information security breaches for listed companies. Our sample includes a large set of cyber attacks between 1995 and 2015; 226 cases of information security breach for 110 companies. Of these 226 cyber attacks, 67 affected 34 financial entities.

We find evidence of an overall negative stock market reaction to public announcements of information security breaches. In the financial sector, we find higher negative market returns than other sectors in the event windows before the cyber risk announcements, especially in asymmetric event windows (-10; -1) and (-5; -1). This may imply that cyber criminals are involved in insider trading. Non-financial companies also show statistical mean CARs in two event windows, (-5; 5) and (-3; 3), after the announcement. Considering the confidential or non-confidential nature of cyber attacks, we find that in general, non-confidential attacks (computer viruses and worms, DOS attacks and system breakdowns) are more dangerous in both financial and non-financial sectors. Moreover, financial entities show greater negative effects on market returns than companies belonging to other economic sectors. Most mean CARs in the financial sector are statistically significant and higher than in other sectors. This is not surprising given that beyond protecting data, banks and other financial entities also have the challenge of safeguarding their systems and networks as well as the financial assets they hold.

Our results have the following implications. Given that cyber attacks determine negative, often very big, falls in market returns, it is extremely important to consider this kind of risk. All companies, especially financial ones, need to equip themselves with efficient control systems, and to do this at an optimal level of investment, they need to understand the true negative impact of information insecurity. Second, we found that cyber crime may be linked to insider trading. It follows that financial authorities need to strengthen cybersecurity measures. Finally, we show that the negative effect on market returns differ according to the event type and the sector of the company. But all companies, especially financial ones, need to prevent cyber attacks, and define levels of priority of different types of threat.

References

Acquisti, A., Friedman, A. & Telang, R. (2006). Is there a cost to privacy breaches? An event study. *Workshop on the Economics of Information Security* (Cambridge, UK).

Allen, F. & Santomero, A.M. (1997). The theory of financial intermediation. *Journal of Banking and Finance*, **21(11-12)**, 1461-1485.

Allen, F. & Santomero, A.M. (2001). What do financial intermediaries do? *Journal of Banking and Finance*, **25(2)**, 271-294.

Anderson, R. (2001). Why information security is hard – an economic perspective. *Annual Computer Security Applications Conference (ACSAC)* (New Orleans, Louisiana), 10-14 December, 358-365.

Andoh-Badoo, F.K. & Osei-Bryson, K.M. (2007). Exploring the characteristics of internet security breaches that impact the market value of breached firms. *Expert Systems with Applications*, **32(3)**, 703-725.

Bener, A.B. (2000). *Risk perception, trust and credibility: a case in Internet banking*. University College of London, London.

Bhattachrya, S. & Thakor, A.V. (1993). Contemporary banking theory. *Journal of Financial Intermediation*, **3(1)**, 2-50.

Boehmer, E., Musumeci, J. & Poulsen, A. (1991). Event-study methodology under conditions of event-induced variance. *Journal of Financial Economics*, **30(2)**, 253-272.

Brockett, P.L., Golden L.L. & Wolman W. (2012). Enterprise cyber risk management. In: *Risk management for the future – Theory and cases*. Emblemsvag, J. (ed.), pp. 319-340. InTech.

Brown, S.J. & Warner, J.B. (1980). Measuring security price performance. *Journal of Financial Economics*, **8(3)**, 205-258.

Campbell, K., Gordon, L., Loeb, M. & Zhou, L. (2003). The economic cost of publicly announced information security breaches: Empirical evidence from the stock market. *Journal of Computer security*, **11(3)**, 431-448.

Campbell, J., Lo, A. & MacKinlay A.C. (1997). *The econometric of financial markets* (Princenton University Press, Princenton, NJ).

Cashell, B., Jackson, W.D., Jickling, M. & Webel, B. (2004). The Economic Impact of Cyber-Attacks. *CRS Report for Congress*. Congressional Research Service.

Cavusoglu, H., Mishra, B. & Raghunathan, S. (2004). The effect of Internet security breach announcements on market value: capital market reactions for breached firms and Internet security developers. *International Journal of Electronic Commerce*, **9(1)**, 69-104.

Cohen, F. (1997a). Information system defences: a preliminary classification scheme. *Computer and Security*, **16(2)**, 94-114.

Cohen, F. (1997b). Information systems attacks: a preliminary classification scheme. *Computer and Security*, **16(1)**, 29-46.

Cohen, F., Phillips, C., Swiler, L.P., Gaylor, T., Leary, P., Rupley, F. & Isler, R. (1998). A cause and effect model of attacks on information systems. *Computer and Security*, **17(1)**, 211-221.

Cooper, M.J., Dimitrov, O. & Rau, P.R. (2001). A rose.com by any other name. *Journal of Finance*, **56(6)**, 2371-2388.

Dos Santos, B.L., Peffers, K. & Mauer, D.C. (1993). The impact of information technology investment announcements on the market value of the firm. *Information Systems Research*, **4(1)**, 1-23.

Fama, E.F., Fisher, L., Jensen, M. & Roll, R. (1969). The adjustement of stock prices to new information. *International Economic Review*, **10(1)**, 1-21.

Eisenstein, E.M. (2008). Identity theft: An exploratory study with implications for marketers. *Journal of Business Research*, **61(11)**, 1160–1172.

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

Garg, A., Curtis, J. & Halper, H. (2003). Quantifying the financial impact of IT security breaches. *Information Management and Computer Security*, **11(2)**, 74-83.

Geers, K. (2010). The Challenge of Cyber Attack Deterrence. *Computer Law & Security Review*, **26(3)**, 298-303.

Gordon, L.A. & Loeb, M.P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security*, **5(4)**, 438-457.

Gordon, L.A., Loeb, M.P. & Lucyshyn W. (2003a). Sharing information on computer systems security: An economic analysis. *Journal of Accounting and Public Policy*, **22(6)**, 461-485.

Gordon, L.A., Loeb, M.P. & Lucyshyn W. (2003b). Information security expenditures and real options: a wait-and-see approach. *Computer Security Journal*, **19(2)**, 1-7.

Gordon L.A., Loeb M.P. & Sohail T. (2010). Market value of voluntary disclosures concerning information security. *MIS Quartely*, **34(3)** ,: 567-694.

Gordon, L.A., Loeb, M.P. & Zhou, L. (2011). The impact of information security breaches: has there been a downward shift in costs? *Journal of Computer Security*, **19(1)**, 33-56.

Gupta, M., Chaturvedi, A.R., Mehta, S. & Valeri, L. (2000). The experimental analysis of information security management issues for online financial services. *The twenty-first international conference on Information systems* (Brisbane, Australia), 667-675.

Hovav, A. & D'Arcy, J. (2003). The impact of denial-of-service attack announcements on the market value of firm. *Risk Management and Insurance Review*, **6(2)**, 97-121.

Hovav, A. & D'Arcy, J. (2004). The impact of virus attack on the market value of firms. *Information System Security*, **13(3)**, 32-40.

Iheagwara, C., Blyth, A. & Singhal, M. (2004). Cost effective management frameworks for intrusion detection systems. *Journal of Computer Security*, **12(5)**, 777-798.

Ishiguro, M., Tanaka, H., Matsuura, I. & Murase, I. (2007). The effect of information security incidents on corporate values in the Japanese stock market. *Workshop on the Economics of Securing Information Infrastructure* (Arlington).

Kahn, C.M. & Roberds, W. (2008). Credit and identity theft. *Journal of Monetary Economics*, **55(2)**, 251–264.

Kannan, A., Rees, J. & Sridhar, S. (2007). Market reaction to information security breach announcements: an empirical analysis. *International Journal of Electronic Commerce*, **12(1)**, 69-91.

Kerschbaum, F., Spafford, E.H. & Zamboni, D. (2002). Using internal sensors and embedded detectors for intrusion detection. *Journal of Computer Security*, **10(1/2)**, 23-70.

Ko, M. & Dorantes, C. (2006). The impact of information security breaches on financial performance of the breached firms: an empirical investigation. *Journal of Information Technology Management*, **27(2)**, 13-22.

Kundur, D., Feng, X., Mashayekh, S., Liu, S., Zourntos, T. & Butler-Purry, K.L. (2011). Towards modelling the impact of cyber attacks on a smart grid. *International Journal of Security and Networks*, **6(1)**, 2-13.

MacKinley, A.C. (1997). Event studies in economics and finance. *Journal of Economic Literature*, **35(1)**, 13-39.

McConnell J.J. & Muscarella, C.J. (1985). Corporate capital expenditure decisions and the market value of the firm. *Journal of Financial Economics*, **13(3)**, 399-422.

Mikkelson, W. & Partch, M. (1988). Withdrawn security offerings. *Journal of Financial and Quantitative Analysis,* **23(2)**, 119-133.

Oates, B. (2001). Cyber Crime: how technology makes it easy and what to do about it. *Information Systems security*, **9(6)**, 1-6.

Odulaja, G.O. & Wada, F. (2012). Assessing Cyber crime and its Impact on E-Banking in Nigeria Using Social Theories. *African Journal of computing & ICTs*, **4(3)**, 69-82.

Pennathur, A.K. (2001). Clicks and bricks: e-Risk Management for banks in the age of the Internet. *Journal of Banking and Finance*, **25(11)**, 2013-2123.

Peterson, P. (1989). Event studies: A review of issues and methodology. *Quarterly Journal of Business and Economics*, **28(3)**, 36-66.

Power, R. (2002). CSI/FBI 2002 Computer Crime and Security Survey. *Computer Security Issues and Trends*, **18(2)**, 7-30.

Shackelford S.J. (2009). From Nuclear War to Net War: Analogizing Cyber Attacks in International Law. *International Law*, **27(1)**, 191-251.

Shackelford S.J. (2012). Should Your Firm Invest in Cyber Risk Insurance? *Business Horizons*, **55(4)**, 349-356.

Sharpe, W. (1963). A simplified portfolio analysis. *Management Science*, **9(2)**, 277-293.

Subramani, M. & Walden, E. (2001). The impact of e-commerce announcements on the market value of firms. *Information Systems Research*, **12(2)**, 135-154.

Winn, J. & Govern, K. (2009). Identity theft: risks and challenges to business of data compromise. *Journal of Science Technology & Environmental Law*, **28(1)** , 49-63.

Appendix

Below, we report the types of cyber attack announced by the sampled companies from 1995 to 2015.

NAICS	**Industry description**	**Type of attack**				
		Unauthorized access to confidential information	*Computer virus and worm*	*DOS attack*	*System breakdown*	**Total**
221118	Other Electric Power Generation		1			**1**
312111	Soft Drink Manufacturing				1	**1**
316211	Rubber and Plastics Footwear Manufacturing	1				**1**
324110	Petroleum Refineries		1			**1**
325412	Pharmaceutical Preparation Manufacturing		1		1	**2**
325620	Toilet Preparation Manufacturing		1			**1**
332312	Fabricated Structural Metal Manufacturing	1				**1**
333315	Photographic and Photocopying Equipment Manufacturing			1		**1**
334111	Electronic Computer Manufacturing		1		3	**4**
334112	Computer Storage Device Manufacturing	1				**1**
334119	Other Computer Peripheral Equipment Manufacturing		1			**1**
334210	Telephone Apparatus Manufacturing	3				**3**
336411	Aircraft Manufacturing	2	3			**5**
336414	Guided Missile and Space Vehicle Manufacturing	1	2		1	**4**
441228	Motorcycle, ATV, and All Other Motor Vehicle Dealers	2	1			**3**
441229	All Other Motor Vehicle Dealers		2			**2**
443120	Computer & Software Stores		2		1	**3**
443142	Electronic Stores			2		**2**
445110	Supermarkets and Other Grocery (Except Convenience) Stores			1		**1**
446110	Pharmacies & Drug Stores	1				**1**
448140	Family Clothing Stores	3				**3**
451120	Hobby, Toy, & Game Stores	1				**1**

451211	Book Stores		1			**1**
452990	All Other General Merchandise Stores	1				**1**
453210	Office Supplies and Stationery Stores	1				**1**
454111	Electronic Shopping	7	1	3	4	**15**
481111	Scheduled Passenger Air Transportation	2	1			**3**
482111	Line-Haul Railroads		1			**1**
492110	Couriers		2			**2**
511110	Newspaper Publishers	1	2	1	2	**6**
511210	Software Publishers	7	9	6	15	**37**
513322	Cellular and Other Wireless Telecommunications	3	4	1		**8**
515210	Cable and Other Subscription Programming	1				**1**
517110	Wired Telecommunications Carriers		1	1	1	**3**
517210	Wireless Telecommunications Carriers	1	1			**2**
517919	All Other Telecommunications	5	4	1	2	**12**
518210	Data Processing & Related Svcs	2	1	2	5	**10**
519130	Internet Publishing and Broadcasting and Web Search Portals			1		**1**
520000	Finance and Insurance	23	10	22	12	**67**
541410	Interior Design Services	2	2			**4**
541511	Custom Computer Programming Services	1	2	1		**4**
541519	Other Computer Related Services		1			**1**
561311	Employment Placement Agencies	1				**1**
561621	Security Systems Services (except Locksmiths)	1				**1**
811213	Communication Equipment Repair and Maintenance				1	**1**
Total		**75**	**59**	**43**	**49**	**226**

Notes: The table shows the composition of the cyber attacks in our sample (i.e.types of cyber attack announced by the sampled companies from 1995 to 2015). Unauthorized accesses to confidential information are confidential attacks and computer viruses and worms, DOS attacks and system breakdowns are non-confidential attacks.