The effect of information security breaches on stock returns: Is the cyber crime a threat to firms?

Maria Cristina Arcuri
Research Fellow, Department of Management, Facoltà di Economia, Università di Roma "La Sapienza",
PhD of "Banking and Insurance", SDA School of Management
Viale Rustici 52, 43123 Parma, Italy
E-mail: mariacristina.arcuri@gmail.com
Phone: +393703085705

Marina Brogi
Full Professor, Department of Management, Facoltà di Economia, Università di Roma "La Sapienza",
Via Bernardino Telesio 17, 20145 Milan, Italy
E-mail: marina.brogi@uniroma1.it
Phone: +393355942276

Gino Gandolfi
Full Professor, Department of Economics, Università degli Studi di Parma,
SDA Professor of "Banking and Insurance" at the SDA School of Management
Via Kennedy 6, 43100 Parma, Italy
E-mail: gino.gandolfi@sdabocconi.it
Phone: +393387364638

Abstract

A very debated issue in recent years is the cyber crime and its impact on market returns and reputation of firms. The issue is made particularly actual by the proliferation of information technology and internet.
Information security breaches are concerned with protecting the accessibility, integrity and confidentiality of information. As a consequence, there are potential high explicit and implicit costs to firms due to these breaches.
This paper investigates the impact of information security breaches on stock returns.
We compiled a broad dataset of cyber attacks which involved firms all over the world. 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 2012. Our main data sources are Factiva and Datastream.
Our expected findings have interesting operating implications, regarding stock market reaction to public announcements of cyber attacks.

EFM Classification: 510, 530, 570

JEL Classification: G10, G15, G20

Keywords: cyber risk, cyber attack, information security, stock market

1. Introduction

Cyber risk has become a very debated issue in recent years. It represents a potential big threat to public and private institutions due to its effects on organizational information systems, reputation and loss of stakeholder's confidence (Brockett et al., 2012). The proliferation of information technology and internet has affected all economic sectors (Gordon et al., 2003). Although internet has often improved the way to conduct business, widespread interconnectivity has increased the vulnerability of the critical infrastructures to information security breaches.
Some studies state that the information security breaches could be quite costly to firms (Garg et al., 2003; Gordon and Loeb, 2002; Gordon et al., 2011). In particular, there are potential explicit and implicit costs to firms due to these breaches (Iheagwara et al., 2004; Kerschbaum et al., 2002). Some survey results (Power, 2002) show that information security breaches cause significant financial losses for firms. Moreover, understanding the true impact of cyber attack on the stock market returns is crucial to decide the investments in information security activities. Therefore, the cyber risk is a very important topic also for banks and other financial institutions.
Several researches (Campbell et al., 2003; Cavusoglu et al., 2004; Hovav and D'Arcy, 2003; Kannan et al., 2004) have examined the impact of announcements of cyber attack on the stock market returns of publicly traded companies. However, the findings from these studies are mixed: the announcements have often, but not always, a significant negative impact.
As far as we are aware, the literature on the economics of information security is rather small [only Gordon and Loeb (2002) and Anderson (2001) examine this aspect] and none study addresses the issue with reference to the financial sector.
The purpose of this paper is to empirically address the following question: *Is the cyber crime a threat to firms?* We examine the stock market reaction to newspaper reports of cyber attacks at listed firms belonging to our sample. First we run an event study to estimate the cyber attack consequences on market returns of the entire sample. Second, we analyse the potential differences between the financial sector and other economic sectors. In summary, we have two main results: first, the stock market returns are influenced by cyber attacks; second, market returns of financial institutions are not negatively affected by information security breach announcements.
The current study examines the issues under investigation over an extended period, 1995-2012.
The remainder of the paper proceeds as follows: in Section 2, we present the literature review; in Section 3 and 4, we describe, respectively, the data and methodology. In Section 5, we discuss our results and in Section 6, we provide concluding comments.

2. Literature review

There are a large number of studies dealing with information security breaches (Dos Santos et al., 1993; Oates, 2001; Vatis, 2001; Gordon and Loeb, 2002; Garg et al., 2003; Gordon et al., 2003; 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; Anderson and Moore, 2008; Eisenstein, 2008; Shackelford, 2008; Winn and Govern, 2009; Geers, 2010; Kundur et al., 2011; Brockett et al., 2012; Odulaja and Wada, 2012; Shackelford, 2012), but literature related to the financial sector is still limited.
An information security breach can have negative economic impacts: lower sales revenues, higher expenses, decrease in future profits and dividends, worse reputation, reduction in the market value (Power, 2002; Gordon et al., 2003). Since the market value represents the confidence that investors have in a firm, measuring the market value allows to calculate the impact of a cyber attack.

Several researches (Campbell et al., 2003; Cavusoglu et al., 2004; Hovav and D'Arcy, 2004) have used the event study methodology to estimate the cyber attacks consequences on the market value of breached firms. The mentioned studies have also considered the type of breach. Campbell et al. (2003) stated that the nature of breach influences CAR, while Cavusoglu et al. (2004) and Hovav and D'Arcy (2004) found that the nature of attack is not a determinant of CAR.

In general, there is a consensus that the announcement of security breach leads to negative Cumulative Abnormal Return (CAR). Campbell et al. (2003) focused on public firms and found a highly significant negative market reaction when breaches are related to unauthorized access to confidential data. Cavusoglu et al. (2004) found that breached firms lost average of 2,1% market value within 2 days of announcement. Acquisti et al. (2006) show that there is a negative and statistically significant impact of data breaches on a company's market value on the announcement day for the breach. Ishiguro et al. (2007) found statistically significant reactions in around 10 days after the news reports and observe that the reaction to news reports of the cyver attacks is slower in the Japanese stock market than in the US market. Gordon et al. (2011) conducted the analysis over two distinct sub-periods and found 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 present a list of sets of attacks, defenses and effects (Cohen, 1997a; Cohen, 1997b; Cohen et al., 1998). Gupta et al. (2000) demonstrate that the attacker's motivations determine the level of attack intensity. Moreover, Bener (2000) notes that investors behavior depend on what they have observed in the past (e.g., investors take decisions considering the impacts of security breaches on the market value of a firm happened in the past).

As far as we are aware, the literature on the economics of information security is rather small. 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 to protect information, a firm should spend only a small fraction of the expected loss due to a security breach. Anderson (2001) put forward a new view of information insecurity: it is due, among others, to network externalities, asymmetric information, moral hazard, adverse selection. Kahn and Roberds (2008) focused on identity theft with reference to the credit transactions. They consider this attack as "the quintessential crime of the information age" and model a tradeoff 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 sector. In particular, they deal with the resources devoted to information security and state that important answers about this issue come from economic analysis.

Overall, the number of researches dealing with information security breaches in the financial industry is limited. The main contribution of our paper is that it presents a comparison between financial and other economic sectors. Information security is a very important issue in financial sector, above all if we consider their potential impact of reputation. Reputation of financial intermediaires is, in fact, crucial consider that the supply of payment, the risk management services and the asymmetric information create systemic risk (Bhattachrya and Thakor, 1993; Allen and Santomero, 1997, 2001). Furthermore, today the online presence of the banking industry is significant (Pennathur, 2001), consequently we have to include the cyber risk among all others banking risks.

The second contribution to the literature is that our paper examines the issues under investigation over an extended period, 1995-2012.

3. Data

We selected our sample by using the Factiva database. In particular, we search newspaper reports of cyber attacks over the period 1995-2012[1]. We insert 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 184 information security breaches (i.e., events). We obtained stock market prices from the Datastream database (the market prices 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. As a result, our final sample includes 128 cyber attacks (events) affecting 81 firms. Of these 128 security breaches, 34 have concerned 17 financial institutions.

Table 1 and Table 2 report the sample industry distribution and the events distribution over the period 1995-2012.

Table 1: Sample industry distribution

NAICS	Industry description	No of firms
312111	Soft Drink Manufacturing	1
316211	Rubber and Plastics Footwear Manufacturing	1
325412	Pharmaceutical Preparation Manufacturing	1
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
33421	Telephone Apparatus Manufacturing	1
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	1
443120	Computer & Software Stores	1
446110	Pharmacies & Drug Stores	1
448140	Family Clothing Stores	2

[1] According to previous literature, we chose 1995 as the beginning date because it coincide with the development of the Internet.

451120	Hobby, Toy, & Game Stores	1
451211	Book Stores	1
453210	Office Supplies and Stationery Stores	1
454111	Electronic Shopping	3
481111	Scheduled Passenger Air Transportation	4
482111	Line-Haul Railroads	1
492110	Couriers	2
511110	Newspaper Publishers	3
511210	Software Publishers	4
513322	Cellular and Other Wireless Telecommunications	2
515210	Cable and Other Subscription Programming	1
517210	Wireless Telecommunications Carriers	1
517919	All Other Telecommunications	4
518210	Data Processing & Related Svcs	4
519130	Internet Publishing and Broadcasting and Web Search Portals	1
52	Finance and Insurance	17
541410	Interior Design Services	2
541511	Custom Computer Programming Services	3
541512	Computer Systems Design Svcs	1
541519	Other computer related services	1
561311	Employment Placement Agencies	1
Total		**81**

Notes: The table shows the sample industry distribution according to the North American Industry Classification System (NAICS).

Table 2: Events distribution over the period 1995-2012

Year	**No of events**	**% of the sample**
1995	1	0,78%
1996	0	
1997	3	2,34%
1998	2	1,56%
1999	20	15,62%
2000	27	21,09%
2001	14	10,94%
2002	5	3,91%
2003	13	10,16%
2004	10	7,80%
2005	11	8,60%
2006	1	0,78%
2007	8	6,25%
2008	2	1,56%
2009	1	0,78%
2010	2	1,56%

2011	4	3,12%
2012	4	3,12%
Total	**128**	

Notes: The table shows the distribution of the cyber attacks announcements over the period 1995-2012.

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. The event study methodology has been widely used in the banking and finance literature (e.g., Brown and Warner, 1980). The implicit assumption is that the financial markets respond to news that affect a security's value, so stock market returns are able to capture the implicit and explicit costs of cyber attacks (Acquisti et al., 2006; McConnell and Muscarella, 1985). In particular, if a firm suffers from information security breach then it may incur financial losses which should reflect in its stock price. Thus, stock prices on the days surrounding the event can capture the impact of that event and measure the economic cost of such cyber attack. Hence, the event study methodology is based on the semi-strong version of the efficient market hypothesis (Fama et al., 1969).

First, we calculate abnormal returns (ARs) that are the 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 by applying OLS-regression methodology for time series of 121 trading days prior to the event window and regressing the daily returns for stock *i* on day *t* ($R_{i,t}$) on returns on market index on day *t* ($R_{m,t}$). The normal return $R_{i,t}$ is measured as follows:

$$R_{i,t} = \alpha_i + \beta_i R_{m,t} + \varepsilon_{i,t} \quad (1)$$

where $R_{j,t}$ is the stock rate of return of the affected company *i* on day *t*, net of the risk free rate (RF_t); $R_{m,t}$ is the rate of return on market index on day *t*, net of the risk free rate (RF_t); α_i is the idiosyncratic risk component of share *i*; β_i is the beta coefficient of share *i* and $\varepsilon_{i,t}$ is the random error. In the light of the broad set of firms encompassed by our sample, we select the following market indexes: the S&P 500 Composite[2], the Nasdaq and the S&P 600 Small Cap. We use the market index total return as our proxy of $R_{m,t}$[3]. Using the firm-specific parameters estimated for the market model over the estimated period, the $AR_{i,t}$ is measured as follows:

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

The event window is defined as the time window that takes into account $-\tau 1$ days before and $+\tau 2$ day after the date of the announcement (the date of the announcement is defined as day zero).

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

[3] Some studies employ a set of control firms in the same industry to assess the Abnormal return (e.g. Cooper et al., 2001).

Following a standard approach, we consider various event windows with different length: (-20; 20), (-10; 10), (-5; 5), (-3; 3) and (-1; 1).

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 (CAR_i) 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 $(\tau 1, \tau 2)$ is the event window.

The average CAR for the event period [$\overline{CAR}\,(\tau 1, \tau 2)$] 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 CAR using the Boehmer et al. (1991) test statistic Z to capture the event-induced increase in return volatility as follows:

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

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:

$$SCAR_{i,t} = \frac{CAR_i\,(\tau 1, \tau 2)}{\sigma_i \sqrt{Ts + Ts\text{^}2/T + \sum_{t=\tau 1}^{\tau 2} (Rm,t - Ts\,\overline{Rm}) / \sum_{i=1}^{t} (Rm,t - \overline{Rm})}} \tag{7}$$

where $\overline{R_m}$ is the average return on market index in the estimation period, σ_i is the estimated standard deviation of AR on stock *i*, T is the number of days in the estimation period, T_s 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.

5. Results

Table 3 presents the results of our analysis. Focusing on the whole sample of information security breaches, we found that the average CARs are negative in all event windows: cyber attacks always lead companies to negative market returns. The statistical significance of mean CAR varies in the event windows. In particular, results display a statistical significance at the 90% confidence level or above. Specifically, the event windows (-20;20), (-10;10), (-5;5), (-3;3) and (-1;1) show mean CARs of -0.029, -0.021, -0.004, 0.012 and -0.003 respectively.

Table 3: Test statistics on CARs for the whole sample

Event window	No of observations	No of firms	Mean CAR	Z-test	% of negative CARs
(-20;20)	128	81	-0.029	-1.045*	51.56
(-10;10)	128	81	-0.021	-1.446*	53.12
(-5;5)	128	81	-0.004	-7.290***	50.78
(-3;3)	128	81	-0.012	-4.282**	53.91
(-1;1)	128	81	-0.003	-4.644***	50.21

Notes: The table reports the result of the event study carried out on the data for 128 cases of cyber attacks announced by 81 listed companies between 1995 and 2012. 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 test statistic Z, reported in Equation (6).
* Statistically significant at 10% (one-tailed test)
** Statistically significant at 5% (one-tailed test)
*** Statistically significant at 1% (one-tailed test)

We also partition the sample based on the economic sector of firms. In particular, we analyse the potential differences between the financial sector and other economic sectors. Table 4 and Table 5 reports our results. We focused on the following event windows (-3;3) and (-1;1).
Considering the financial sector (Table 4), we found that the average CARs are positive in the two event windows (0.019 and 0.006 respectively), showing that cyber attack announcements do not lead financial institutions to negative market returns. The mean CAR is significantly positive only for the event window (-1;1).
Focusing on the other economic sectors (Table 5), we found that the average CARs are negative in the two event windows (-0.023 and -0.006 respectively), showing that information breach announcements lead firms to negative market returns. The mean CAR is significantly negative both for the event window (-3;3) and also for the event window (-1;1).
These results suggest that only the market returns of firms belonging to other economic sectors are negatively affected by the cyber attack announcements. Our findings are consistent with previous literature: the announcements have often, but not always, a significant negative impact.

Table 4: Test statistics on CARs for the financial entities

Event window	No of observations	No of firms	Mean CAR	Z-test	% of negative CARs
(-3;3)	34	17	0.019	1.113	44.12
(-1;1)	34	17	0.006	3.188***	35.29

Notes: The table reports the result of the event study carried out on the data for 34 cases of cyber attacks announced by 17 listed financial companies between 1995 and 2012. 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 test statistic Z, reported in Equation (6).
* 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 the other sectors

Event window	No of observations	No of firms	Mean CAR	Z-test	% of negative CARs
(-3;3)	94	66	-0.023	-2.111***	53.91
(-1;1)	94	66	-0.006	-5.293***	50.78

Notes: The table reports the result of the event study carried out on the data for 94 cases of cyber attacks announced by 66 listed companies between 1995 and 2012. 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 test statistic Z, reported in Equation (6).
* Statistically significant at 10% (one-tailed test)
** Statistically significant at 5% (one-tailed test)
*** Statistically significant at 1% (one-tailed test)

6. Conclusions

In this study, we estimated market returns consequences for listed companies following the announcement of information security breaches. We conduct our analysis over an extended period, 1995-2012. We consider a broad set of firms. In particular, our sample encompasses 128 cyber attacks affecting 81 firms; of these 128 security breaches, 34 have concerned 17 financial institutions.

We found that the announcements of cyber attacks affect the stock market returns. In particular, we found evidence of an overall negative stock market reaction to public announcements of information security breaches.

We partition our sample based on the economic sector of firms in order to analyse the potential differences between the financial sector and other economic sectors. We found that only the market returns of firms belonging to other economic sectors are negatively affected by the cyber attack announcements. In fact, the other economic sectors showed negative mean CARs in the event windows (-3;3) and (-1;1), while financial sector showed positive mean CARs in the same event windows.

Our results have interesting operating implications. First, we found that cyber attack announcements affect stock market returns of firms. Consequently, understanding the true impact of cyber attack on the stock market returns is crucial to decide the investments in information security activities. The issue is made particularly actual by the proliferation of information technology and internet. Second, we showed that stock market reaction differs according to the economic sector of firms. As such, above all some firms need to equip themselves with control systems that monitor exposure to cyber risk, in order to reduce financial and reputational losses.

Many aspects of the analysed issue deserve however to be further investigated. Among them, the potential consequences of the different information security breaches and the potential damage on reputation of firms.

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. In Proceeding of 17th Annual Computer Security Applications Conference (ACSAC), New Orleans, Louisiana.

Anderson, R.,, Moore, T., 2008. Information Security Economics – and Beyond. In Deontic Logic in Computer Science - Lecture note in computer science 5076, 49.

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, 703-725.

Bener, A.B., 2000. Risk perception, trust and credibility: a case in Internet banking. London: London Schooll of Economics and Political Sciences.

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, 253-272.

Brockett, P.L., Golden L.L., Wolman W., 2012. Enterprise cyber risk management, in Risk management for the future – Theory and cases, Jan Emblemsvag.

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, 431-448.

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, 69-104.

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

Cohen, F., 1997b. Information systems attacks: a preliminary classification scheme. Computer and Security 16, 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, 1-23.

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

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

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

Garg, A., Curtis, J., Halper, H., 2003. Quantifying the financial impact of IT security breaches. Information Management and Computer Security 11, 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, 438-457.

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

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

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, 33-56.

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

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, 97-121.

Hovav, A., D'Arcy, J., 2004. The impact of virus attak 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, 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. In Workshop on the Economics of Securing Information Infrastructure, Arlington.

Kahn, C.M., Roberds, W., 2008. Credit and identity theft. Journal of Monetary Economics 55, 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, 69-91.

Kerschbaum, F., Spafford, E.H., Zamboni, D., 2002. Embedded sensors and detectors for intrusion detection. Journal of Computer Security 10, 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, 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.

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

Mikkelson, W., Partch, M., 1988. Withdrawn security offerings. Journal of Financial and Quantitative Analysis 23, 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 (2), 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, 2013-2123.

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

Shackelford S.J., 2008. 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, 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.

Vatis, M.A., 2001. Cyber attacks during the war on terrorism: a predictive analysis. Institute for security technology studies at Datmouth College.

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.