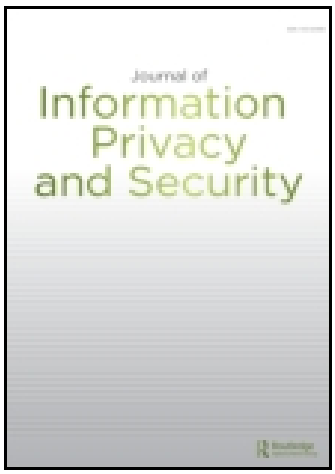


Journal of Information Privacy and Security
Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/uips20

Stock Market Response to Information Security Breach: A Study Using Firm and Attack Characteristics

Saini Das[a], Arunabha Mukhopadhyay[b] & Manoj Anand[c]
[a] Indian Institute of Management, Lucknow, India,
[b] Indian Institute of Management, Lucknow, India,
[c] Indian Institute of Management, Lucknow, India,
Published online: 07 Jul 2014.

To cite this article: Saini Das, Arunabha Mukhopadhyay & Manoj Anand (2012) Stock Market Response to Information Security Breach: A Study Using Firm and Attack Characteristics, Journal of Information Privacy and Security, 8:4, 27-55, DOI: 10.1080/15536548.2012.10845665

To link to this article: http://dx.doi.org/10.1080/15536548.2012.10845665

Stock Market Response to Information Security Breach: A Study Using Firm and Attack Characteristics

Saini Das, Indian Institute of Management, Lucknow, India, fpm9009@iiml.ac.in

Arunabha Mukhopadhyay, Indian Institute of Management, Lucknow, India, arunabha@iiml.ac.in

Manoj Anand, Indian Institute of Management, Lucknow, India, manand@iiml.ac.in

ABSTRACT

The recent global surge in information security breaches emphasizes the importance of their impact determination for proper risk assessment. In this paper we used event study to compute the cumulative abnormal response (CAR) of the stock market to publicly announced breaches on a sample of Indian and US firms. We also used linear regression and moderation analysis to identify the factors that affect CAR individually and in combination with each other. From regression analysis, firm type, firm size and Damage Potency of the attack emerged as factors that individually impacted CAR. Further, moderation analysis revealed that Denial of Service attacks on e-commerce companies and information theft attacks on BFSI companies generated significantly negative CAR. We also observed that if a subsidiary company is breached, then the parent's stock market performance is not significantly negatively impacted. However, if a vendor suffers a breach, then the client is significantly negatively affected in the stock market.

KEY WORDS

Information Security Breach, Denial-of-service Attacks (DoS), Information Theft, Cumulative Abnormal Return, E-commerce Companies, Moderation Analysis.

INTRODUCTION

The incidence of information theft rose from 18% in 2009 to 27.3% in 2010. Banking, financial services and insurance (BFSI) companies reported the highest incidence of information and electronic data theft in 2010 (Economist Intelligence Unit and Kroll, 2010). Annually, large e-commerce based businesses suffered losses of up to US$30 million in direct revenue and reduced productivity due to cyber breaches (Prolexic Technologies, 2011). On average, businesses lost $1.7 million to cyber-fraud for every billion dollars of revenue they earned (Economist Intelligence Unit and Kroll, 2010). The 2010 Computer Crime and Security Survey reported a non-linear trend followed by all types of cyber breaches namely, viruses, worms, Trojan horses, spams, Denial-of-service (DoS), phishing, and confidentiality thefts from 1997 to 2010. In 2010,

there was a huge increase in the incidence of malware infections, DoS, password sniffing and website defacement attacks, whereas 2009 saw a rise only in malware, bots and phishing attacks (Computer Security Institute, 2010).

These findings suggest that it is very important for organizations which are electronically networked, to ensure information security. Information security struggles with protecting the confidentiality, integrity and availability (CIA) of information (National Institute of Technical Standards, 1995). But even the best efforts to prevent security breaches may not always succeed because of the novelty and uncertainty of the attack. Thus, it is extremely important to assess the risk of a cyber attack to enable companies to take relevant measures as a means of preventing potential damages. However, it is very difficult to find adequate historical data to calculate the likelihood and impact of information security risk (U.S G.A. Office, 1999). Hence, as a first step, it is important to determine the impact of information security breaches on organizations.

Many studies exist that investigate various aspects of cyber security attacks. In this paper we determine the stock market reaction to publicly declared cyber attacks on listed e-commerce, BFSI and other companies. We achieved this by calculating the Cumulative Abnormal Return (CAR) generated by using standard event study (ES) methodology. CAR is the sum of differences between the expected return (computed using Capital Asset Pricing Model) on a stock and the actual return up to a particular point in time. CAR is used to assess the impact of an external event on the stock price of a firm. We also performed regression analysis to find out how various attack specific (i.e., type of attack and it's damage potency) and firm specific characteristics (i.e., firm type, size and performance) affect the CAR. We then performed moderation analysis using Analysis of variance (ANOVA) to determine the combination of firm-specific and attack-specific characteristics that would lead to high negative stock market returns. This study can help companies decide what precautions should be taken and exactly where to invest in order to minimize the damage caused by an attack

This paper is structured as follows. In Section 2, we provide review of related work in this field. In Section 3, we introduce our model and explain its related factors. In Section 4, we discuss the source of the data for our study. Section 5 details the methodology used in this study. In Section 6 we show the results. Discussion and concluding remarks are found in Section 7.

RELATED WORK

Several studies have been conducted regarding the impact, risk and severity associated with a cyber attack on an organization. Most of these studies focused on finding the economic cost of a publicly announced cyber attack on an organization by determining the abnormal returns of the company in the stock market as a result of the declaration(Campbell et al. 2003; Goel & Shawky 2009; Chen et al. 2011; Hovav & D'Arcy 2003; Hovav & D'Arcy 2005; Cavusoglu et al. 2004).

Campbell et al (2003) conducted an event study analysis (ESA) on publicly traded US corporations to examine the stock market reaction to publicly announced information security breaches. They found that there was a highly negative market reaction for attacks that involved a breach of confidential information, but no such negative reaction for attacks that did not involve a breach of confidential information. Cavusoglu et al (2004) also employed ESA to study the impact of internet security breaches on market values of affected firms. They found that firms lose approximately 2.1% of their market value or $1.65 billion of market capitalization per incident; they also found that market values of security solution developers, on average, increased 1.36% more than that expected by the market model, or $1.06 billion over a two-day event period. Also, the study revealed that firm type, firm size and nature of attack affected the market value of the firm suffering from the attack. In another ESA, Goel and Shawky (2009) found that on an average, the announcement of a corporate security breach negatively impacted the market value of the firm by about 1% during the days of the event.

Hovav and D'Arcy (2003) conducted an ESA on the impact of DoS attack announcements on market values of firms. They found that the market reacts negatively and penalizes "internet-specific" companies that heavily rely on the web. However, they concluded that the reaction is not true for companies that do not largely rely on the web. Hence, large companies which are not "internet-specific" may be overly cautious by investing resources to prevent a DoS attack problem that may have a marginal impact on their shareholder value. Hovav and D'Arcy (2005) later conducted another ESA to determine the impact of virus attack announcements on the market value of the firm. They found that the market does not penalize companies affected by such attacks. Chai et al (2010) focused on risk assessment of information security investment decisions. They noted that an information security investment leads to positive returns for firms.

Chen et al (2011) assessed the severity of phishing attacks through the inherent risk level of the attacks and the CAR of the stock price of the targeted firm during the period of the event. The relevant financial data related to targeted firms and the text phrases extracted from the phishing mails using text mining were used as input variables to predict the severity of the attack with up to 89% accuracy. Park et al (2007) classified worm attacks into various impact categories using two parameters namely, (i) total life impact of the worm (Total hit number, Hit density and damage Potency) and (ii) short term life impact of the firm (skewness, early time period hit number and damage potency). Table 1 gives a summary of previous research findings in this area.

Table 1. Summary of Previous Research Findings

Researchers	Type of Attack	Antecedents of CAR	Finding
Campbell et al. (2003)	All announced IS Breaches	Attack Type	Breaches involving unauthorized access to confidential information result in a loss of firm value of 5.5%
Hovav & D'Arcy (2003)	DoS attack announcements	Firm type	Market reacts negatively and penalizes "internet-specific" companies
Cavusoglu et al. (2004)	All announced IS Breaches	Firm type, Firm size, Attack type	Firms lose 2.1% of their market value or $1.65 billion of market capitalization within two days after the breach. Security solution developers gain 1.36% more than that expected by the market over a two-day event period
Gatzlaff & McCullough (2010)	All announced IS Breaches	Market-to-book ratios, Firm Size, Subsidiary Status	Overall statistically significant negative impact of attacks.
Garg et al. (2003)	All announced IS Breaches		Each security breach incident costs companies between $17 and $28 million or .5%-1% of annual sales
Hovav & D'Arcy (2005)	Virus attacks		Market does not penalize companies affected by viruses
Goel & Shawky (2009)	All announced IS Breaches		Market value of the firm negatively impacted by about 1% during the days surrounding the event.
Chai et al. (2010)	IT security investment announcements		IS investment leads to positive abnormal returns for firms.

Based on the review of literature, we noted that the direction of the stock market reaction to publicly announced cyber attacks on listed companies was ambiguous. Firm specific and attack specific parameters like (i) firm size, (ii) firm type, (iii) attack type and (iv) damage potency of the cyber attack affect the market value of the firm.

This can be measured in terms of the CAR of the stock prices of the targeted firms during the period of the attack. Until now, most work in this field has focused on CAR determination to assess the stock market impact of cyber breaches. Our paper bolsters this field of study by determining the combination of attack specific (i.e., type of attack) and firm specific characteristics (i.e., firm type) that lead to high negative CAR.

THEORETICAL FRAMEWORK AND HYPOTHESIS DEVELOPMENT

Our paper proposed to assess the impact of a cyber attack based on Crockford's Risk-Components (CRC) Model that revealed the impact of any threat on firm performance. According to the CRC model, threats may compromise resources of a firm and thus negatively impact market value or earnings. Some moderating factors like firm size and IT resources also augment the impact of a threat on stock market performance of a firm (Crockford, 1986; Chen et al., 2011).

Figure 1 shows our proposed severity analysis model (SAM) for assessing the impact of a security threat on firm performance. An information security breach can compromise IT assets and confidential information of an organization. It can also congest the entire network. This impact on the IT resources directly affects the financials (i.e., market capitalization, total assets) and intangibles (i.e., brand image and reputation) of the organization. The public announcement of such a breach indirectly affects the stock market performance of the firm. We have used CAR as an indicator to measure the firms' responses to the attack and the subsequent market response.

In this model we have determined the extent of compromise resulting from a security breach on an organization by analyzing the combined effect of attack-specific characteristics (i.e., type of attack and it's damage potency) and firm-specific characteristics (i.e., firm type, size and performance) on the firm's stock market performance.

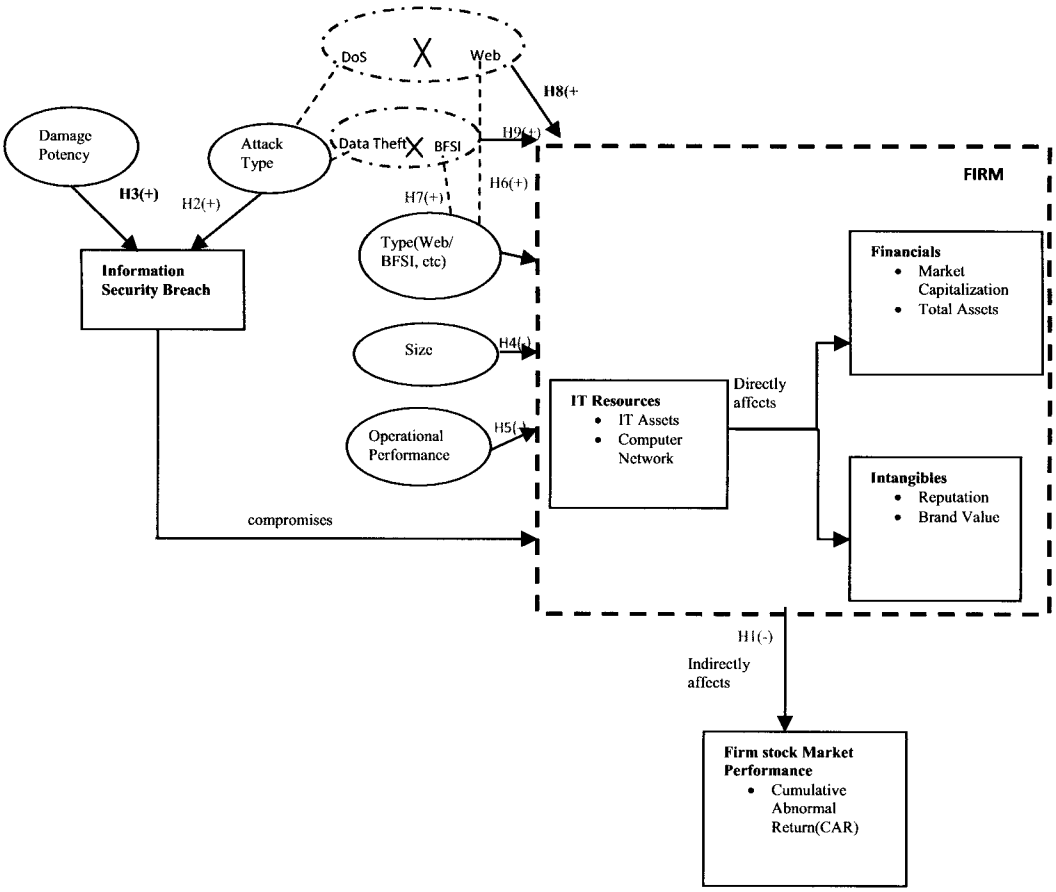


Figure 1. Proposed Severity Analysis Model (SAM) [where, → causality; X=interaction]

The plain black ellipses in Figure 1 represent the factors that individually affect CAR whereas the dashed and dotted ellipses with crosses represent interaction effect of two factors on CAR. Most of the previous studies in this field found that public declarations of information security breaches on listed companies led to abnormal CAR (Garg et al., 2003; Cavusoglu et al., 2004; Goel & Shawky, 2009). Therefore we also hypothesize that:

H1: Public announcements of corporate information security breaches on listed firms lead to negative CAR in the stock market.

The following section describes factors used in Figure 1 and derives the hypotheses to be tested.

Type of Attack

It is observed that customers, stockholders and other stakeholders of a company are more concerned about theft of confidential information compared to DoS attacks, virus attacks or other information security breaches (Campbell et al. 2003; Hovav & D'Arcy 2003; Hovav & D'Arcy 2005). Hence, we can hypothesize that:

H2: The CAR (negative) due to an internet security breach is higher for theft of confidential information than other breaches.

Damage Potency

Damage Potency (DP) measures the intrinsic effects of a cyber attack to cause detriment to an organization, especially its IT assets (Park et al. 2007). DP of a cyber breach is classified into five types by McAfee (a major antivirus vendor) (McAfee (n.d.)). Table 2 shows the classification of DP in decreasing order of severity.

Table 2. Damage Potency Levels

DP Level	Coded as	Description/Impact	Attack Category	Violation of (C/I/A)?		
				C	I	A
Unforeseeable	5	Destruction of an entire network	U2R, DoS	Y	Y	Y
Very Serious	4	Data/files compromised, manipulated & sent to third party	U2R, R2L	Y	Y	Y
Serious	3	Formats hard drive, Deletes/modifies/copies important files; System recovered using specific tools, Unauthorized access to sensitive information; Malware injection.	U2R, R2L	Y	Y	Y
Medium	2	Generates medium amount of network traffic; Renders the network temporarily unavailable	DoS			Y
Little	1	No major system changes; Imitation of bogus texts/sounds Deletion of less significant files; Damage recovered easily	Probe, R2L		Y	

U2R = User to Root; R2L = Remote to Local; DoS = Denial of Service; C = Confidentiality; I = Integrity; A = Availability

Each attack is classified into a particular DP level by matching similar words or synonyms present in the attack description provided in the newspaper article and the information provided in the "Description/Impact" field of Table 2. Table 3 classifies the information security breaches in our dataset into their inherent DP level. The words in bold and within quotation marks in the "Attack Description from Newspaper article" column of Table 3 are aligned with the meanings in the "Description/Impact" field of Table 2.

Table 3. Categorization of Sample Attacks According to the Damage Potency

Firm Name	Type of Attack	Attack Description from Newspaper Article	Damage Potency
Yahoo	DDoS attack	**"Network rendered unavailable temporarily"** for a few hours in each attack scenario.	Medium
Amazon(1)*			
eBay Inc			
Amazon(2)**			
ICICI bank(1)*	Phishing attack/unauthorized access	Website cloning and **"sensitive data manipulation"**	Very serious
Bank of India	Website hacked, malware injected	**"Malware injected"**	Serious
ICICI Bank(2)**	Phishing attack/unauthorized access	Accesses and **"modifies sensitive info"** like login, password, account info and credit card data.	Very serious
Axis bank	Phishing attack	**"Attempt to access sensitive confidential information"**	Serious
PNB	Malware attack	**"Malware attack"** damaged many computers	Serious
Infosys	Virus attack	Unknown virus attack that **"brought the operations to a grinding halt for few hours"**	Medium
Bharti Airtel	Unauthorized access to sensitive information	**"Hacking sensitive personal information"**	Very serious
Intel	Website hacked	Website hacked, **"not much damage"**	Little

PNB = Punjab National Bank; * (1) First attack on a company, **(2) Second attack on the same company

Since an information security breach with Very Serious DP can be extremely severe, it can cause significant negative stock market returns for the firm (Park et al., 2007). Accordingly, we formed the following hypothesis:

H3: The CAR (negative) is higher for an information security breach of very serious DP.

Organization Factors

Several organizational or firm-specific factors play an important role in determining the impact of an information security breach. Several variables pertaining to the firm were initially deemed as important. However, by using the expertise of a financial specialist, 7 financial variables were classified into two firm-specific factors namely, size of the firm (Chen et al, 2011; Cavusoglu et al, 2004) and operating performance of the firm.

Size of the Firm

Size of the firm is an extremely important parameter in determining the impact of a cyber attack. Larger firms are usually better equipped to deal with cyber attacks as a result of financial status (i.e., greater access to capital markets, more capital to deal with, diversified product markets, trusted brand names), better slack resources to be used in case of a security breach and better skilled IT personnel (Cavusoglu et al, 2004). Accordingly, the following hypothesis emerges:

H4: The CAR (negative) due to information security breach is larger for smaller firms.

The variables that determine the size of a firm are identified as: invested capital, total assets, intangibles and total receivables. Invested capital represents the total cash investment that shareholders and debt-holders have made in a company. The invested capital in form of share capital, reserves and surplus (net worth) determines the size of an organization. Total assets, or the value of all assets (current and fixed), determine the size of an organization (Nyamache, 2010). The company size is also found to be positively related to the extent of disclosure on intangibles in the annual report. Hence intangibles are an indicator of firm size (Arvidsson, 2003). The total receivables of an organization also determine firm size.

Operating Performance of the Firm

Higher profit firms are understood as better performing firms. A profit maximizing firm generally makes an optimum level of investment in information security and attempts to eliminate sources of operational risk (Lee et al., 2011). Operational risks include risks that evolve with daily business operations of the organization. IT risks are categorized as operational risks which include customer satisfaction, product failure, integrity and reputational risk (Casualty Actuarial Society, 2003). Hence,

better performing companies are better equipped to deter and prevent cyber breaches (Ernst and Young, 2010). Based on this, we formed the following hypothesis:

H5: The CAR (negative) due to information security breach is larger for firms with smaller revenue earnings.

The two variables that determine the operating performance of the firm are total revenue and earnings before interest and tax (EBIT). EBIT is an important indicator of a firm's operational performance (Lasher, 2003). Total Revenue is also an important indicator of firm performance (Jin et al., 2004).

Type of Industry

The type of industry is another firm-specific characteristic that determines the impact of a cyber attack. We considered firms from two sectors: internet dependent or web firms and BFSI firms, as these are the worst affected in cases of information security breaches. Web firms (like eBay and Amazon), also called pure play or internet specific firms, are those that depend entirely on the internet for all transactions and business (Cavusoglu et al., 2004). Information security breaches on such companies also lead to loss of reputation, legal suits and loss of confidential data. Integrity (I) and confidentiality (C) of data are very important for such firms. The stock market reacts negatively and penalizes such companies most as a result of a security breach (Hovav and D'Arcy, 2003). On the other hand, the non internet-specific (non e-commerce) firms that are less dependent on the web are less affected by cyber attacks (Cavusoglu et al., 2004). Another distinction can be made between BFSI (banking, financial services and insurance companies) and non-BFSI companies regarding the impact of cyber attacks. Generally, BFSI companies which have plenty of confidential information like customer PIN, SSN, credit card data etc., are lucrative targets for financially-motivated cyber attackers (Choo, 2011). In this study, the industry types are classified into three types:

1. BFSI companies

2. Internet-specific companies (Hovav & D'Arcy, 2003; Cavusoglu et al., 2004).

3. Other (non BFSI and non Internet-specific) companies belonging to various sectors.

From the previous observations we hypothesize that:

H6: As a result of information security breaches, the CAR (negative) is greater for internet-specific firms compared to that of the sample population without internet-specific firms.

H7: The CAR (negative) due to information security breach is larger for BFSI companies compared to that of the sample population without BFSI companies.

In this paper we also consider a combination or interaction of some firm-specific and attack-specific factors that might have a significant impact on CAR. Such effect is also called moderation. In such a scenario, a third variable might affect the direction/strength of relationship between an independent variable and a dependent variable (Barron and Kenny, 1986). If a DoS attack occurs on an internet-specific company then the negative impact of the attack on the firm might increase manifold (Hovav and D'Arcy, 2003). For such companies, outages due to DoS attacks translate into revenue and opportunity loss because customers would not be able to make purchases online during that period. In turn, such companies would lose reliability and sway customers to other organizations. This would result in loss of reputation. Similarly, if confidentiality theft happens at a BFSI company, then the negative impact of the attack on the firm might increase significantly. Data breach/confidentiality theft attacks would lead to loss of sensitive information and reputation. Organized criminals often use such sensitive information for committing fraud like launching phishing campaigns or committing identity theft. Eventually all such activities lead to financial gains for the attackers. (Verizon Report, 2012). Therefore, the industry type plays the role of a moderator between the independent variable, attack type, and dependent variable, CAR. Hence, we hypothesize that:

H8: CAR (negative) due to DoS attack is larger for internet-specific firms as compared to non- internet-specific firms.

H9: CAR (negative) due to data breach/confidentiality theft attack is greater for BFSI companies compared to non BFSI companies.

DATA SOURCE

Many sources exist that provide information on various aspects of cyber security attacks (Steinke, Tundera and Kelly, 2011).

Table 4. Sample Data of Information Security Breach Incidents

Industry Type	Firm Name	Stock Exchange	CI (million USD)	Date of Declaration	DP	Violation of (C/I/A)?		
						C	I	A
Internet-specific	Yahoo	NASDAQ	29	7/2/2000	Medium			Y
	Amazon		2568	8/2/2000				
	eBay Inc		3789	9/2/2000				
BFSI	ICICI bank	NSE	37430	10/2/2006	Very serious	Y		
	Axis bank		11063	19/12/2006	Serious			
	Citigroup	NYSE	501220	22/12/2009	Very serious	Y		
he Retail	TJX	NYSE	5492	17/1/2007	Very serious	Y	Y	Y

		Wal-Mart		154712	24/12/2009	Medium			Y
	Oil and Gas	ONGC	NSE	18466	23/11/2008	Little	Y		
		ExxonMobil	NYSE	341461	25/1/2010	Medium	Y		
		Conoco Phillip		83295					
	IT/ITeS	Infosys	NSE	722	29/6/2004	Medium	Y		
		MphasiS		125	12/4/2005	Very serious	Y		

Our data sources were newspaper and internet declarations of 101 information security breaches on companies listed on the NYSE (US), NASDAQ (US) or NSE (India). We searched by the keywords: "information security breach," "data breach," "website hacked," "phishing attacks," "website defacement" etc.

Table 5. Classification of BSFI and Internet-specific Companies in our Sample

Banking firms		Examples from our sample	Internet-specific companies		Examples from sample
BFSI	Banking companies	Bank of America	**Internet-specific Companies**		AT&T
		Bank of New York Mellon(BNYM)			Adobe
		National Bank of Blacksburg(NBB)			IBM
		ICICI Bank			Verisign
		State Bank of India			EMC
		Punjab National Bank			Google
		Axis Bank			Yahoo
		IDBI bank			LinkedIn
		HDFC bank			eBay
		United Bank of India			Amazon.com
		Bank of India			Futurebazaar
		Union Bank of India			Zappos
	Financial Service Companies	Citigroup			Paypal
		Keycorp			Apple
		Fidelity national Financial			Sony
		Morgan Stanley			
		Heartland Payment Systems			
		Global Payments Inc.			

		Mastercard		
		VISA		
		American Express		
		Discover Card		
		JP Morgan chase		
	Insurance	Progressive Corporation		

The data was collected over a 12 year period, (i.e., 2000 to 2012) from wire feeds of ABIInform and Lexis Nexis databases, and included 101 attack declarations. 71 breaches were reported by US companies, and the remaining 30 by Indian companies.

We ensured that there were no other significant events like mergers, acquisitions, earnings, stock splits, etc. within the firm during the period of the cyber breach declaration. Table 4 shows the sample data of information security breach incidents included in our study. The financial data for the Indian and US companies were obtained from Prowess/Capitaline databases (www.capitaline.com) and company annual reports/Google Finance/Yahoo Finance websites, respectively. This data was collected from the Annual Report of the year prior to the announcement of each attack. The BSFI companies and internet-specific companies in our sample can further be classified as shown in Table 5.

RESEARCH METHODOLOGY

We used event study methodology (ESA) approach in order to compute the CAR of stock prices in the event of announcements of an internet security breach at a firm. CAR is used as the dependent variable in this study as it determines the change in stock price of the firm due to the market sentiments resulting from the cyber attack, such as loss of clients, market share reduction and reduced confidence from consumers and investors (Chen et al., 2011).

The computation procedure of CAR is based on the capital asset pricing model (CAPM). CAPM assumes a linear relationship between the return of the market portfolio and the individual security, as shown in Equation 1.

$$R_{it} = \alpha_i + \beta_i R_{mt} + \varepsilon_{it} \quad \ldots(1)$$

where, R_{it} = return of stock i on day t; R_{mt}= return on the market portfolio on day t, α_i, β_i = intercept and slope parameter for firm I; ε_{it} = disturbance term for stock i on day t with the usual OLS properties.

Our estimation period ranges from 122 days to 2 days prior to the cyber attack announcement. We used the NYSE/NASDAQ/NIFTY market index return as our proxy for R_{mt} depending on the respective stock exchange in which a particular

company is listed. R_{it} for each firm is obtained from stock price data in the corresponding stock exchange. We used the coefficient estimates, α, β, from market model regression in Equation 1, to predict the expected return over the event window. The abnormal return (AR) for the firm i on the day t of the event window is computed using Equation 2.

$$AR_{it} = R_{it} - (a_i + b_i R_{mt}) \quad \ldots(2)$$

where a_i and b_i represent the parameter estimates obtained by regressing R_{it} against R_{mt} over the 120 days estimation period prior to the event announcement. AR represents the extent to which the actual returns (R_{it}) on the event period deviate from the expected returns ($a_i + b_i R_{mt}$).

To capture the stock market effect of an announcement of a cyber attack, we used a three day event window centered on the date of the cyber attack declaration. This window captures the market reaction that may occur on the date of the announcement, as well as any that may occur on the previous or subsequent day. It is important to include the day before the cyber breach in order to include any reaction that may occur due to leakage of information, or to report a reaction about an attack that may begin on a certain day but may not be publicized until the following. Investors may take 1-2 trading days to fully realize the consequence of the announcement. In certain cases the impact on the stock market may be stretched over a period of 3-4 days after the attack. Hence, we also considered a five day event window ranging from one day prior to the attack, to three days after the attack and calculated the CAR for the period. Then we can compare the CARs for the event windows (-1,1) and (-1,3) to check whether there is any further drop in stock market return over a period of three days after the attack compared to one day after the attack. The CAR over the event window is calculated as shown in Equation 3.

$$CAR_i = \sum_{t=1}^{t} AR_{it} \quad \ldots(3)$$

Where t = (-1,1) is one day before the cyber attack announcement to one day after it, and t = (-1,3) is one day before the cyber attack announcement to three days after it. A short event window is preferred to a long one in order to eliminate the impact of other unrelated events like change in government policies, mergers and acquisitions that may lead to false statistical inference (McWilliams & Siegel, 1997). For our sample of 101 cyber attack announcements, we computed the mean announcement effect as shown in Equation 4.

$$CAR = \frac{1}{N} \sum_{i=1}^{N} CAR_i \quad \ldots(4)$$

where, N = the number of cyber attack announcements.

To test the hypothesis that mean CAR over the event period was significantly different from zero, we use student' s t- test, which is shown in equation (5).

$$t = \frac{CAR}{\sqrt{var(CAR)}} \sim t_{(\alpha, df = N-1)} \quad \ldots(5)$$

We then perform a regression analysis to find out how various (i) attack specific (i.e., type of attack and its damage potency) and (ii) firm specific characteristics (i.e., firm type, size and performance) individually affect the CAR generated. We also perform Analysis of Variance (ANOVA) to determine the combination or interaction of firm-specific and attack-specific characteristics that would lead to high negative stock market returns.

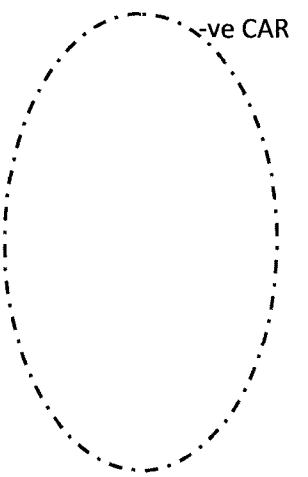
DATA ANALYSIS AND RESULTS

Descriptive and Statistics Analysis of CAR

We categorized the CAR into four groups: significantly positive, moderately positive, moderately negative and significantly negative, as shown in Table 6.

Table 6. Range of Values for Different CAR Categories

CAR categories	Range of Values (%)
Significantly Negative (SN)	< -3
Moderately negative (MN)	-3 to 0
Moderately positive (MP)	0 to +3
Significantly Positive (SP)	> 3



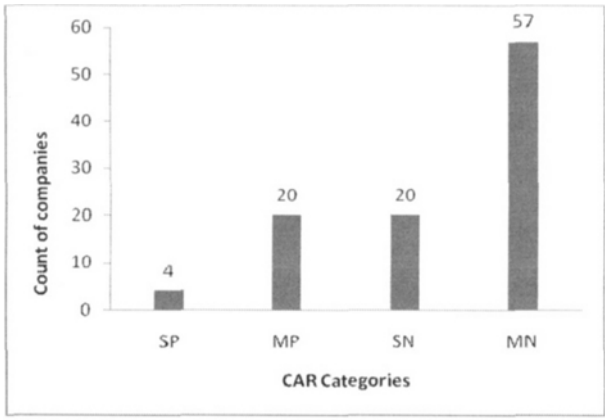
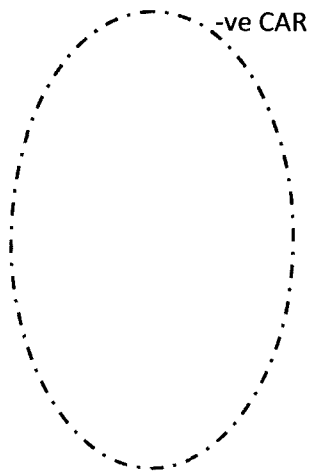


Figure 2a. Distribution of CAR Generated by the Cyber Attacks during the Event Window (-1, 1)

Figure 2a and 2b show the distribution of the CARs generated for the event windows (-1, 1) and (-1, 3) respectively. The value of the t-statistic for the CAR (calculated using Eq. 5) was -.254 which is not statistically significant. Hence we do not find support for hypothesis H1. This is in line with the findings of Campbell et al. (2002) and Hovav and D'Arcy (2005). However, there is partial support for H1 as more than half of the firms (76 out of 101 during the three day window (-1, 1) (from Figure 2a) and 68 out of 101 during the five day window (-1, 3) (from Figure 2b) experienced negative abnormal returns due to the attacks. Hence, we conducted further analysis on the data to find out relevant factors that affect the CAR for the event window (-1, 1).



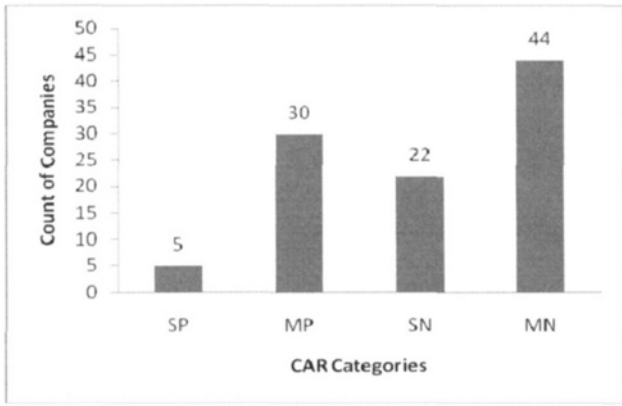


Figure 2b. Distribution of CAR Generated by the Cyber Attacks during the Event Window (-1, 3)

Table 7 shows the CAR for a few companies from our dataset for event periods (-1, 1) and (-1, 3). The sample had relevant CAR data for the event window (-1, 1) that ranged from -14.71 (Global Payments Inc.) to 8.23 (MphasiS) with a mean of -1.15 and a standard deviation of 3.31. For event window (-1, 3), the CAR data ranged from -50.29 (Heartland Payment System) to 8.57 with a mean of -.1.51 and a standard deviation of 5.94. The values of the t-statistics for the mean CAR are -0.347 and -0.254, respectively, for event windows (-1, 1) and (-1, 3). These values are not statistically significant. For event window (-1, 3), the CAR data ranged from -50.29 (Heartland Payment System) to 8.56 (MphasiS) with a mean of -.1.51 and a standard deviation of 5.94.

Table 7. CAR for Sample Companies for the Event Periods (-1, 1) and (-1, 3)

Company	Event Period		Company	Event Period	
	(-1, 1)	(-1, 3)		(-1, 1)	(-1, 3)
Yahoo	-4.85	-10.63	eBay Inc.	-8.46	-11.39
Heartland PS	-13.75	**-50.29**	Futurebazaar	-0.99	-5.16
Global Payment	**-14.71**	-11.7	MphasiS	**8.23**	**8.57**
Sony	-5.59	-8.45	Nokia	-3.1	-4.74
Novartis	-0.540	-0.80	**Sample Mean**	**-1.15**	**-1.51**
Bank of America	-1.54	-1.99	**Sample St dev.**	**3.31**	**5.94**

Factor Determining the Variance of CARs

The final independent variables are (i) capital invested (CI), (ii) total assets (TA), (iii) EBIT and (iv) total revenue (TR), (v) firm type (FT), (vi) attack type (AT) and (vii) damage potency (DP). We dropped two variables, i.e. total receivables and intangibles, from further analysis due to lack of data. The CAR for the event window (-1, 1) was used as the dependent variable in our study. We performed two different sets of analysis, scenario (A) for internet-specific/non internet-specific companies and scenario (B) for BFSI/non-BFSI companies.

Table 8a. Correlation Matrix in Scenario (A)

Variables	CI	EBIT	DP	FT	TA	TR	AT
CI	1						
EBIT	-.01	1					
DP	.27 (**)	.16	1				
FT	-.09	-.05	-.05	1			
TA	.39 (**)	.87 (**)	.27 (**)	-.08	1		
TR	-.02	.99 (**)	.15	-.04	.86 (**)	1	
AT	-.15	.09	.76 (**)	-.15	.15	.07	1

** $p < 0.01$, * $p < 0.05$

Table 8a shows the results of the correlation analysis between the independent variables in scenario (A) and Table 8b shows the results of the correlation analysis between the independent variables in scenario (B).

Table 8b. Correlation Matrix in Scenario (B)

Variables	CI	EBIT	DP	FT	TA	TR	AT
CI	1						
EBIT	-.01	1					
DP	.27 (**)	-.06	1				
FT	.29 (**)	-.05	.29 (**)	1			
TA	.39	.87	.27	.11	1		

	(**)	(**)	(**)				
TR	-.02	.99 (**)	.15	-.04	.86 (**)	1	
AT	-.15	.09	.76 (**)	-.15	.15	.07	1

** $p < 0.01$, * $p < 0.05$

CI = Capital Invested , EBIT = Earnings before interest and tax, DP = Damage Potency, FT = Firm Type, TA = Total Assets, TR = Total Revenue, AT = Attack Type

In both cases, TA had a very high significant positive correlation ($p < 0.01$) with both EBIT and TR. Hence this variable was dropped from further analysis. AT had a high significant correlation with DP. Hence, it is also dropped from further analysis. So, we find no support for hypothesis H2. Further, EBIT and TR had a very high significant positive correlation with each other. We dropped TR from further consideration since EBIT is a better indicator of firm performance than revenue. In scenario (B), FT had a mild significant positive correlation ($p < 0.05$) with DP. But since the correlation was not very strong we considered both the variables for further analysis.

An ordinary least square regression analysis was performed on the two scenarios to test the hypotheses (H2-H7). The regression model is shown in Equation 6:

$CAR_i = \alpha + \beta_1$Firm size (Capital Invested) + β_2Firm Performance (EBIT) + β_3 Damage Potency + β_4Firm type (internet-specific/non internet-specific or BFSI/non BFSI) ...(6)

In our initial regression model, EBIT emerged as a highly insignificant variable. We dropped it and performed a regression with three independent variables, namely, CI, DP and FT. Hence we do not find support for hypothesis H5. Table 9a shows the

results for scenario (A) and Table 9b shows the results for scenario (B). Scenario (A) has a significant F-value of 4.493 with R^2 of 0.123 and an adjusted R^2 of 0.096. The coefficient for CI is positive and significant (t = 2.129, p-value =0.036). This means that firms with lower CI have more negative abnormal return in case of a cyber attack when compared with firms that have higher CI.

Since CI determines the size of the firm, this means that a larger firm is less affected in the stock market by a cyber attack than a smaller firm. This supports hypothesis H4. DP emerges as a significant variable (t = -2.725, p-value = 0.008). This shows that cyber attacks with serious and very serious damage potency cause significantly higher abnormal returns in the stock market. This supports hypothesis H3. The coefficient for FT is moderately significant (t =-1.966, p-value = 0.052).

Table 9a. Regression Analysis Results (Scenario A)

Variables	Coefficient	Standard Error	t-statistic	p-value
Constant		1.651	-0.844	0.401
CI	0.754	0.354	2.129	0.036
DP	-0.013	0.361	-2.725	0.008
FT	-1.569	0.798	-1.966	0.052
R^2	-1.73			
Adjusted R^2	0.096			
F-value	4.493			

Table 9b. Regression Analysis Results (Scenario B)

Variables	Coefficient	Standard Error	t-statistic	p-value
Constant		1.738	-1.178	0.242
CI	0.803	0.378	2.213	0.036
DP	-0.907	0.382	-2.375	0.02
FT	-0.036	0.745	-0.048	0.961
R^2	0.115			
Adjusted R^2	0.061			
F-value	3.148			

This shows that CAR for cyber security breaches is larger for internet-specific companies. Thus, hypothesis H6 is supported. Scenario (B) has a significant F-value of 3.148. R^2 value is 0.09 and adjusted R^2 is 0.061. The coefficient for CI is again

positive and significant (t= 2.213, p-value= 0.036). This supports hypothesis H4. DP again emerges as a significant variable (t = -2.375, p-value = 0.020). Hence, hypothesis H3 is supported. However, FT does not emerge as a significant variable (p-value = 0.961). Thus, hypothesis H7 is not supported by this sample dataset. ANOVA was performed to test Hypotheses H8 and H9. The regression model for moderation or interaction effect is shown in Equation 7.

$$CARi = b_0 + b_1 \text{Attack Type (AT)} + b_2 \text{Firm type(FT)} + b_3(\text{AT X FT}) \quad \ldots(7)$$

Table 10a shows the results of the ANOVA for the moderation effect .of FT = "internet-specific" on the relationship between AT = "DoS' and CAR. Though AT (DoS) and FT (internet-specific) are individually not significant, their combined effect plays a moderately significant role (0.06) in determining CAR. Hence we find partial support for Hypothesis H8. Table 10b shows the results of the ANOVA for the moderation effect of FT = "BFSI" on the relationship between AT = "Data breach/Confidentiality theft' and CAR. Though AT (Data Breach) and FT (BFSI) are individually not significant, their combined effect plays a significant role (0.038) in determining CAR. Hence we find support for Hypothesis H9.

Table 10a. Results of Moderation Effect for DoS Attack on Internet-Specific Firms

Independent variables	Coefficient	F value	Sig
AT (DoS)	2.18	0.06	0.807
FT(Internet-specific)	4.39	2.069	0.154
AT X FT	-5.01	3.62	0.060

Table 10b. Results of Moderation Effect for Data Breach Attack on BFSI Firms

Independent variables	Coefficient	F value	Sig
AT (Data breach)	2.8	0.667	0.416
FT(BFSI)	1.8	0.032	0.857
AT X FT	-4.03	4.42	0.038

A summary of the results of all the hypotheses tests are shown in Table 11.

Table 11. Summary of Findings

Hypothesis	**Description**	**Supported(Y/N)?**

$H1_0$	Public announcements of corporate information security breaches lead to negative CAR	Partially Supported
H2	CAR due to IS breach is higher for theft of confidential information than other breaches.	N
H3	CAR is higher for an IS breach of very serious damage potency.	Y
H4	CAR due to IS breach is larger for smaller firms.	Y
H5	CAR due to IS breach is larger for firms with smaller revenue earnings.	Y
H6	CAR due to IS breach is larger for internet-specific firms.	Y
H7	CAR (negative) due to IS breach is larger for BFSI companies.	N
H8	CAR (negative) due to DoS attack is larger for internet-specific firms.	Partially Supported
H9	CAR (negative) due to data breach/confidentiality theft attack is larger for BFSI firms.	Y

IS = Information Security

From the regression analysis, the three significant parameters that determine the variance in CAR are CI, DP and FT (internet-specific/non internet-specific). Figure 3 shows a plot of the logarithm of CI by an internet-specific firm against the DP of any attack on it. Attacks of medium and serious DP on e-commerce companies having medium to high CI generated moderately negative abnormal responses in the stock market. Apple, Paypal (subsidiary of eBay) and Google lay in this cluster. It can also be inferred that small and medium (SME) sized internet-specific companies with low invested capital are prone to high severity attacks (such as DDoS and DoS) of medium DP. The maximum negative CAR of -8.457 was generated by the DDoS attack on eBay which had medium CI. A significantly high negative CAR of -4.85 was generated by the same DDoS attack on Yahoo which had much less CI. Hence, we determined that DoS type attacks on internet-specific companies with low to medium CI are extremely severe and can lead to significantly high negative abnormal stock market responses. This is likely because such attacks make their sites inactive for several hours and hamper online transactions. So, financially, such attacks lead to huge losses in revenue and customer confidence of the internet-specific companies.

eBay suffered greater losses compared to Yahoo because most of eBay's revenue comes from online e-commerce activities whereas Yahoo's revenue comes from other sources. In the Indian context, we observe that a DoS attack on Futurebazaar's website led to negative abnormal return of -0.9898 which is less compared to that of eBay and

Yahoo. This is because Futurebazaar is a subsidiary of the FutureGroup which includes large companies like the Pantaloons. Futurebazaar may represent only a small fraction of the company's stock value. Similar is the reason why a confidentiality theft attack of serious DP on Zappos.com (subsidiary of Amazon) resulted in a significant positive CAR of 6.3.

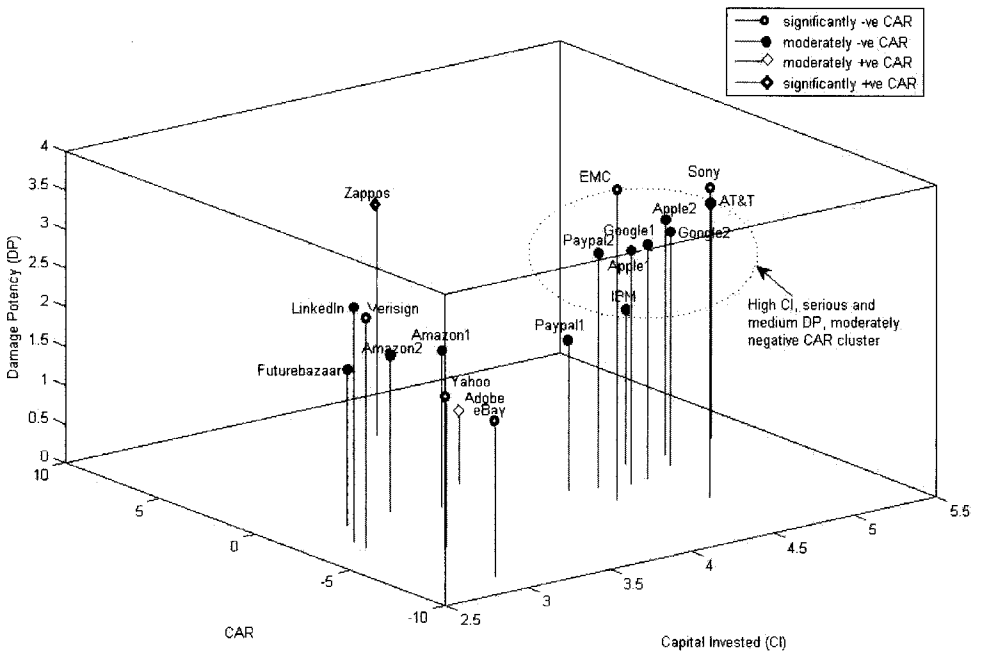


Figure 3. Categorization of Attacks into CAR Generated Based on Capital Invested and Firm Type

Market Response of Cyber Security on Subsidiaries of Large Companies

Ownership status is a firm-specific factor that might influence the stock market response of cyber attacks on a firm. In cases where the victim firm is a wholly owned subsidiary, the parent company's financials are used to determine the stock market impact of the attack (Gatzlaff and McCullough, 2010). We gathered a sample of eight such companies and analyzed the stock market response to cyber breaches on them. Figure 4 shows a plot of the CI of each parent company against the DP of each attack on the subsidiary. Only 3 out of the 8 attacks of serious and very serious DP had generated significantly negative abnormal stock market responses (represented by black triangles), and 2 had moderately negative CAR (represented by black rectangles). The remaining had positive CAR. We reasoned that owner firms which experienced a breach at the subsidiary level, are somewhat insulated and do not bear the direct brunt of the attack. Hence their stock market influence is muted or reduced (Gatzlaff and McCullough, 2010).

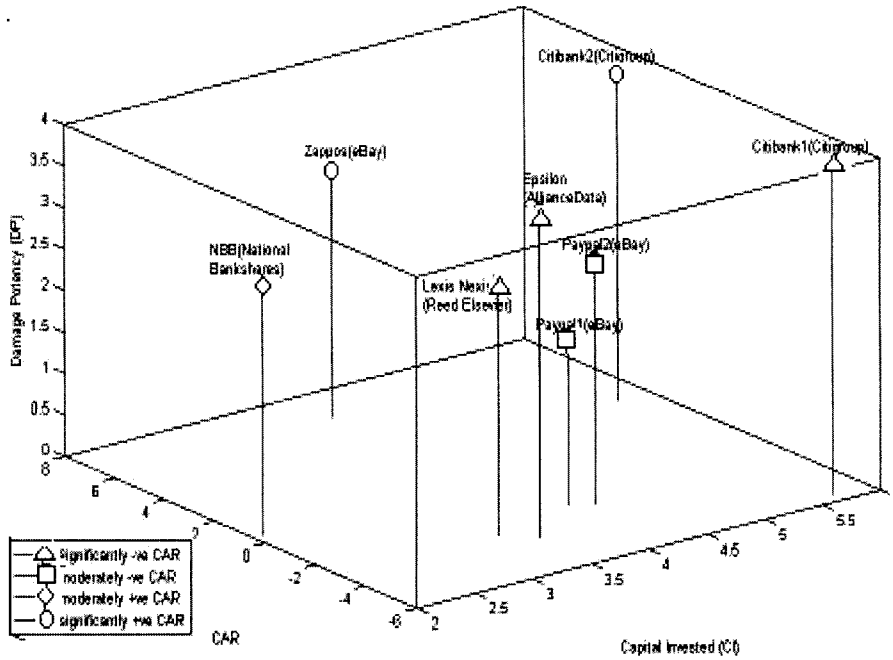


Figure 4. Market Response of Cyber Security Breaches on Subsidiaries of Parent Companies (in Parentheses)

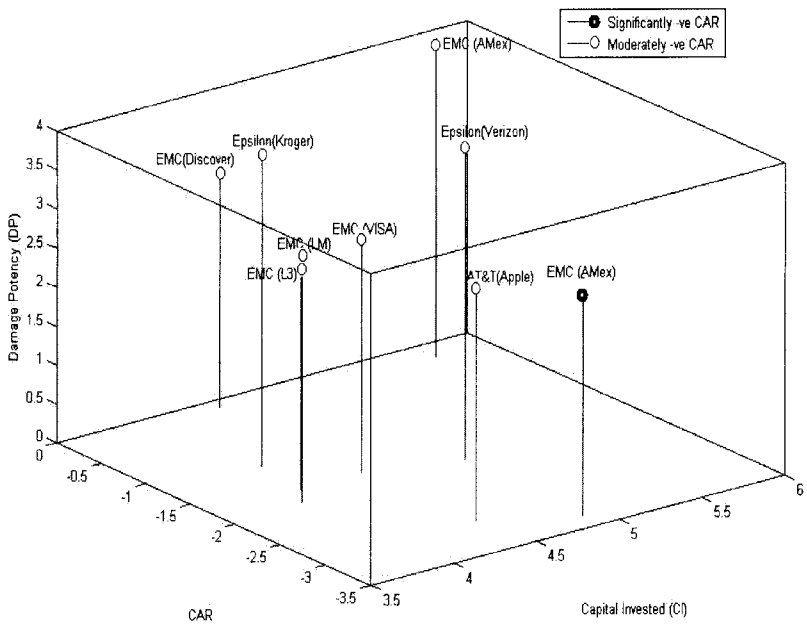


Figure 5. Market Response of Cyber Security Breaches on Vendors of Client Companies (in Parentheses)

Market Response of Cyber Security Breaches on Vendors of Large Companies

If there is a cyber security breach on a vendor of a client company, the client might be adversely impacted in the stock market. We gathered a sample of eight such companies and analyzed the stock market responses to cyber breaches on them. Figure 5 shows a plot of the CI of each client company against the DP of each attack on the vendor. We found that attacks of serious and very serious DP on vendors of client companies having high CI had negative abnormal stock market returns. This emphasizes the need for client companies to not only monitor and validate their own security policies but also those of their vendors (Data protection and Breach Readiness Guide, 2010). This also highlights the fact that vendor selection and relationship is a very crucial business decision for every client.

DISCUSSION AND CONCLUSION

Information security breaches affect a large number of organizations today. We have attempted to understand the severity of a cyber breach on an organization by analyzing the combined impact of (i) attack specific (i.e., type of attack and it's DP) and (ii) firm specific characteristics (i.e., firm type, size and performance) of 101 cyber attack announcements on stock market performance of companies across various sectors. In our sample set we found some evidence of negative CAR to

publicly announced cyber attacks. This is in line with previous work (Campbell et al. 2003; Goel & Shawky 2009; Cavusoglu et al. 2004). However, not all the CARs are statistically significant.

Based on our SAM model we concluded that stock market response to a publicly announced cyber attack on a company is primarily dependent on, (i) company size (capital invested) and (ii) firm type (internet-specific/non internet-specific) and (iii) DP of the attack. The CAR due to information security breach for smaller and internet-specific firms is larger than others. Also attacks of serious and very serious DP (theft of confidential information) result in higher negative CAR. From our study, we determined that DoS attacks on e-commerce companies and data breach/confidentiality theft attacks on BFSI companies generated higher negative abnormal response in the stock market compared to similar attacks on companies belonging to other sectors. We also observed that if a subsidiary company is breached, then the parent's stock market performance is not significantly negatively impacted. However, if a vendor company suffers a breach, then the client is significantly negatively affected in the stock market.

From the managerial perspective, we propose that medium to large sized internet-specific companies should take proper precautions against attacks of medium DP, such as, DOS attacks. Also, large BFSI companies should take precautionary measures against attacks of high DP including data breaches. Moreover, client companies should periodically monitor and validate the cyber security policies of their

existing vendors and include such policies as criterion while selecting their vendors. From the research perspective this study adds to the body of literature already existing in the field, by determining the impact of the stock market on those companies who publicly announce an information security breach. This study identifies how some firm specific and attack specific factors affect the CAR individually as well as in combination. This study attempts to determine the stock market impact of a parent company whose subsidiary suffered a breach and that of a client company whose vendor suffered a breach.

The combination of US and Indian companies in our dataset is a novelty of this study. We also endeavored to find a combination of some attack-specific (attack type) and firm-specific (firm type) factors that affect the CAR of the firm affected by the cyber breach. Moreover, we have also attempted to determine the stock market impact of a client company whose vendor suffered a cyber breach. A limitation of this study is that we could calculate CAR only for publicized cyber attacks on private listed companies. Future work could address the impact of such attacks on government institutions, both nationally and internationally.

Results of this preliminary study should be interpreted with caution. The sample size is small, though studies with this kind of sample size have been done in the past. The combination of US and Indian companies in our dataset is a novelty of this study.

Park (2004) though mentions that the use of the single country market model in a multi-country event study sometimes can overestimate changes in parameters, demonstrating the need for a world market model. Our future research could investigate this aspect of research. Also we have tried to find a combination of some attack-specific (attack type) and firm-specific (firm type) factors that would affect the CAR of the firm affected by the cyber breach. Moreover, we have also attempted to determine the stock market impact of a client company whose vendor suffered a cyber breach. Another limitation of this study is that the event study methodology calculates CAR only for publicized cyber attacks on private listed companies. However, there are a lot of cyber attacks on government companies and there is no way to determine their severity.

ACKNOWLEDGEMENT

The authors acknowledge many good suggestions given by the reviewers which helped to improve the quality of the paper.

REFERENCES

Arvidsson, S. (2003). The Extent of Disclosure on Intangibles in Annual Reports. Paper presented at the *4th Annual SNEE Congress*, May, Mölle.

Barron., K., & Kenny, D. (1986). The Moderator-Mediator Variable Distinction in Social Psychological Research: Conceptual, Strategic and Statistical Considerations. *Journal of Personality and Social Psychology,* 51(6), 1173-1182.

Choo, K. R. (2011). Trends and Issues in Crime and Criminal Justice No. 408. Australian Government and Australian Institute of Criminology.

Campbell, K., Gordon, L., Loeb, M., and 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.

Capitaline database site retrieved from: www.capitaline.com on 23-07-2012

Casualty Actuarial Society. (2003). Overview of Enterprise Risk Management. Retrieved from www.casact.org/area/erm/**overview**.pdf on 21-07-2012.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The Effect of Internet Security Breach Announcements on Market Value of Breached Firms and Internet Security Developers. *International Journal of Electronic Commerce*, **9** (1), 69–104.

Chai, S., Kim, M., & Rao, H.R. (2011). Firms' Information Security Investment Decisions: Stock Market Evidence of Investors' Behaviour. *Decision Support Systems,* **50** (4), 651–661.

Chen, X., Bose, I., Leung, A., & Guo, C. (2011). Assessing the Severity of Phishing Attacks: A Hybrid Data Mining Approach. *Decision Support Systems,* **50**(4), 662-672.

Computer Security Institute. (2010). CSI Computer Crime and Security Survey. San Francisco: Computer Security Institute Inc.

Crockford, N. (1986). An Introduction to Risk Management. Woodhead-Faulkner, Cambridge.

Economist Intelligence Unit and Kroll. (2010). Global Fraud Report. Retrieved from http://www.managementthinking.eiu.com/sites/default/files/downloads/KRL_FraudReport2011-12_US.PDF on 24-07-2012.

Ernst and Young (2011). Countering Cyber Attacks, Insights on IT Risks. Retrieved from http://www.ey.com/Publication/vwLUAssets/Countering_cyber_attacks/$FILE/Countering_cyber_attacks_March2011.pdf on 19-07-2012.

G.A. Office, (1999). Information Security Risk Assessment, in: A.a.I.M. Division (Ed.)", (General Accounting Office) 1-48.

Gatzlaff, K,. & McCullough, K. (2010). The Effect of Data Breaches on Shareholder Wealth. *Risk Management & Insurance Review,* 13(1), 61-83.

Garg, A., Curtis, J., & Halper., H. (2003). Quantifying the Financial Impact of IT Security Breaches. *Information Management and Computer Security,* 11(2/3), 74-83.

Goel, S., & Shawky, H.A. (2009). Estimating the Market Impact of Security Breach Announcements on Firm Values. *Information and Management,* **46**, 404-410.

Google finance site : http://www.google.com/finance retrieved on 30-07-2012.
"Guidelines for the AVERT Risk Assessment" retrieved from http://us.mcafee.com/VirusInfo/VIL/risk_assessment.asp retrieved on 29-07-2012.

Hovav, A., & D'arcy, J. (2003). The Impact of Denial-of-service Attack Announcements on the Market Value of Firms. *Risk Management and Insurance Review,* **6** (2), 97–121.

Hovav, A., & D'arcy, J. (2005). The impact of virus attack announcements on the market value of firms. *Information Systems Security,*13 (3), 32–40.

Jin, Z., Dehuan, J., & Zhigang, F. (2004). The Impact of Business Restructuring on Firm Performance-evidence from Publicly Traded Firms in China. *Academy of Accounting and Financial Studies Journal*, **8** (3)

Lasher. W. (2003). Practical Financial Management. Mason, Ohio: Thomson/South-Western.

Lee, Y., Kauffman, R., & Sougstad, R. (2011). Profit-maximizing Firm Investments in Customer Information Security. *Decision Support Systems,* **51,** 904-920.

McWilliams, A., & Siegel, D. (1997). Event Studies in Management Research: Theoretical and Empirical Issues. *Academy of Management Journal,* 40 (3), 626–657.

Mishra, B.K. and Saini, H. (2009). Cyber Attack Classification using Game Theoretic Weighted Metrics Approach. *World Applied Sciences Journal* **7** *(Special Issue of Computer and IT)*, 206-215.

NIST (National Institute of Technical Standards). (1995). An Introduction to Computer Security: the NIST Handbook. Special Publication 80-12.

Nyamache. J. (2010). Factors that Determine the Size of Business. Retrieved from http://www.docstoc.com/docs/35135761/Factors-That-Determine-The-Size-Of-Business on 19-07-2012.

Online Trust Alliance (OTA). (2012). 2012 Data Protection & Breach Readiness Guide. Retrieved from otalliance.org/resources/incident/2012DataBreachGuide.pdf on 22-07-2012.

Park, I., Sharman, R., Rao, H.R., & Upadhyay, S. (2007). Short Term and Total Life Impact Analysis of Email Worms in Computer Systems. *Decision Support Systems,* 43, 827–841.

Park, N.K. (2004). A Guide To Using Event Study Methods In Multi-Country Settings, *Strategic Management Journal*, 25 (7), 655–668, July 2004.

Prolexic Technologies, Inc. (2011). Defending Against DDoS Attacks:Human Security Mitigation vs. Automated Mitigation. Prolexic White Paper Series. Retrieved from http://www.prolexic.com/kcresources/white-paper/human-security-mitigation-vs.-automated-mitigation-prolexic-white-paper-_A4_082412.pdf on 02/12/2012.

Stanley, N. (2010). The Ongoing Security Paradox. Retrieved from http://www.mcafee.com/us/resources/reports/rp-security-paradox.pdf on 29/11/2012.

Steinke, G., Tundera, E. and Kelly, K. (2011). Towards an Understanding of Web Application Security Threats and Incidents, Journal of Information Privacy and security 7(4), 54-69.

Verizon .(2012). Data Breach Investigations Report. Retrieved from http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf on 17/11/2012.