Cloud Computing Security Announcements: Assessment of Investors' Reaction

Srikanth Parameswaran[1, 2], Srikanth Venkatesan[1] & Manish Gupta[1]

[1]Management Science and Systems, SUNY Buffalo, NY 14260
{sparames[2], svenkate, mgupta3}@buffalo.edu)

Abstract

Security and availability risks have become one of the biggest challenges for firms that are transitioning into the cloud and for firms offering the cloud services as well. Security issues have gained prominence in recent years due to the unprecedented growth in Cloud computing service offerings and their adoption. An event of a security breach may impact investors' perceptions of a firm's value. In fact, prior studies have shown that information security breaches and countermeasures have a significant impact on the firm's stock price. Thus, publicly announcing breach and countermeasures is one way by which firms manage these issues related to cloud security. The focus of this paper is to use event study methodology to investigate how cloud security breach and countermeasures announcements affect the firm and its competitor's stock price. Our research shows that cloud security breach announcements have significant negative impact on the firms and its competitor's stock value. Surprisingly, cloud security countermeasure announcements have significant negative impact on the firm and the competitor's stock value.

Key words: Cloud Computing, Cloud Security, Market Valuation, Investor Reaction, Cloud Security Announcement, Security Breach, Security Investments, Framing effects

[2] Corresponding Author

INTRODUCTION

The arrival of cloud computing has commoditized computing power and empowered computers. It has ushered in an era of the pay-as-you-go model in the computing environment of firms. It provides firms especially SMBs (Expansion), benefit from low cost of entry and reduced IT barriers (Marston et al., 2011). The companies that use these services cite the potential reduction in costs and business agility as primary reasons for their success (Fogarty, 2010; Pemmaraju, 2010). It is not surprising that the adoption of cloud computing has increased over the years. In fact, a study from Ovum has found that the uptake of cloud services among MNCs (Multi-National Company) has grown more than 60 percent since spring 2010 with 45 percent of the MNCs surveyed saying that they have used cloud sourcing for at least some elements of key IT services (Molony and Kirchheime, 2011). Going with this upward trend in the adoption of cloud computing services, the future also looks bright, with Gartner predicting the cloud computing business to be worth $150 billion by 2014. However, as the adoption of cloud computing has increased, there has been a concern over the security and privacy of user data (Heiser and Nicolet, 2008).

Cloud security has become a leading concern for businesses transitioning into the cloud, especially for the healthcare and financial industries that store and use sensitive data. The risks stemming from ensuring availability are transferred to cloud service providers. The risks of additional exposure to entities outside the organization environment are still an unsettled issue (Brodkin, 2008; Heiser and Nicolett, 2008; Mather et al., 2009). According to a survey conducted by Symantec (2011), in 5300 organizations across 30 countries in 2011, organizations rated security as a major concern when moving to the cloud. Though 87 percent of the respondents in the survey were confident that moving into the cloud will actually improve their security, they still felt that achieving security in a cloud environment was their topmost priority, citing potential risks like malware, hacker-based theft, and loss of confidential data (Symantec, 2011). Moreover, the lack of the three essential components of policies, procedures and tools to ensure that sensitive information stored by means of cloud computing hosts remains secure, contributes to the security concerns in the cloud.

Since security in the cloud has emerged as a major concern in cloud adoption, there is sufficient motivation for cloud service providers to invest and better manage cloud security issues. Publicly announcing breach and countermeasures is one way by which firms manage these issues related to cloud security. Organizations attempt to manage issues by means of news media coverage because customers and other external stakeholders pay close attention to issues surrounding a company through media. News media is important for companies to get the attention and influence the perception of the customers and stakeholders (Carroll and Maxwell, 2003; Chen and Meindl, 1991; Deephouse, 2000; Dutton and Dukerich, 1991). There are several studies that have investigated impact of security breaches on stock performance (see for example, Hasan and Yurcik, 2006; Goel and Shawky, 2009; Liginlal et al, 2009; Acquisti et al, 2006; Kark et al.,2008; Campbell et al, 2003; Hovav and Darcy, 2003; Garg et al., 2003a). There has been an increase in the number of news articles related

to security in the cloud computing domain over the past few years to sense whether organizations' have any incentives to disclose breaches and to safeguard their confidential data and their customers' personal information (Acquisti, et al., 2006; Parameswaran et al. 2012). The focus of this paper is to investigate how cloud security breach and countermeasures announcements in media affect the stock price of firms.

Our research explores the impact of announcements of such events on the stock price of the involved firms. We collected 223 announcements made by the firms that faced a cloud security breach. We performed event studies to analyze the stock impact of firms making two kinds of announcements largely; 1. Cloud security breach announcements and 2. Countermeasure announcements which attempt to restore image and reputation after a security breach. We compared the research by Gupta (2010) on the stock impact of information security breaches with the market impact of cloud security breaches obtained from our data. This study also analyzed the effect of company size (in terms of employee strength) on the stock impact of the firms. We have also investigated how cloud security breach and countermeasures announcements by a company affect stock performance of its competitors. Further, content analysis was performed on the cloud security announcement articles to examine the impact of the use of certain frames in writing cloud security breach announcement articles on stock price.

Though there are many studies that analyze information security announcements, a very few of them study the impact of cloud security announcements. This is the first study that analyzes the impact of cloud security announcements on firm valuation. Our study contributes to the existing literature by answering the following research questions:

1. Does the stock market make notice of cloud security announcements?
2. How do cloud security announcements affect the stock prices of competitors of the companies involved in the announcement?
3. What is effect of company size on the stock impact of cloud security breach announcements?
4. How do cloud security announcements affect the stock prices of companies when compared to information security announcements?
5. What is the stock impact of using certain frames in the cloud security announcement articles?

The rest of the paper is organized as follows: Section 2 provides background and literature review in the area followed by the research model, Section 3 discusses the methodology of this research in detail, followed by presentation of the results in Section 4, followed by the analysis of framing effects in Section 5, Section 6 concludes the paper with implications and Section 7 gives limitations and directions for future research.

RESEARCH BACKGROUND AND MODEL

Cloud computing is a model for enabling network access on demand to a pool of computing resources like storage, applications and services that are remotely and conveniently configurable. The resources can be availed rapidly with a service provider interaction (Mell, 2011). Since the concept of cloud computing has changed the way data is stored and shared across interconnected infrastructures, new kinds of security and privacy related issues such as loss of governance, isolation failure, compliance risks, under-provisioning, over-provisioning, distributed denial of service attack (DDoS), economic denial of service attack (EdoS), etc have to be addressed. For example, the concept of multi-tenancy, wherein a single instance of a software program may service multiple tenants or clients, demands proper isolation of users' data. Therefore, a failure in the mechanism that separates the memory, storage and routing between different tenants may be considered a risk that is attributable to the cloud computing environment (Catteddu and Hogben, 2009).

Cloud Security

There are several studies that have focused on issues, frameworks, models and strategies for managing cloud security. Gartner, in its assessment, has identified 7 major security issues, namely privileged user access, regulatory compliance, data location, data segregation, recovery, investigative support and long-term viability (Heiser and Nicolet, 2008). Kavitha and Subashini (2011) present a survey of the security risks of the three types of delivery models namely SaaS, IaaS and PaaS. Ramgovind et al. (2010) which highlight the key security challenges and considerations in cloud computing and suggest guiding principles for managing security in the cloud. Marston et al., (2011) in their SWOT Analysis of cloud computing, point out that organizations should be wary of the loss of control of data put in the cloud, and vendors cannot guarantee the exact location of the organization's data. According to them, the biggest threat to adoption of cloud computing will be the regulation on data privacy, data access, audit requirements and data location requirements at the local, national and international levels. Chen et al. (2010) argue that, though cloud computing raises a lot of security concerns, only two facets are new and fundamental to cloud computing. The two facets are the complexities arising from multi-party trust considerations and the attention to need for mutual auditability. Jensen et al. (2009) present cloud security issues like XML signature, browser security, cloud integrity and binding issues and flooding attacks. According to their study, improving the security capabilities of web browsers and web service frameworks and integrating these web service frameworks into web browsers would be a good direction towards improving the cloud security. Che et al. (2011) survey existing cloud security models and identify the security risks confronted by customers, providers and government. In their paper, they suggest a few strategies to overcome these security risks of cloud computing. Yildiz et al. (2009) proposed a practical security model on the basis of key

security considerations after looking at various infrastructure aspects of cloud computing. Yu et al. (2010) propose a data access control scheme for cloud computing for simultaneously achieving fine-graininess, scalability and data confidentiality.

Security Breaches

Security breaches and their announcements have significant adverse impact on a firm's market valuation. The breached firms, on average lose 2.1 percent of their market value within two days of the security breach announcement, which translates to loss of about $1.65 billion per breach in market value of the firm (Cavusoglu, et al., 2004). Privacy Rights ClearingHouse (Privacy Rights Clearinghouse, 2011) reports 535 data breaches in 2011 with around 30.4 million records containing sensitive personal information being compromised. Cloud security breaches have been on a rise as cloud computing has started to get attention. A Trend Micro survey conducted on May 2011 involving IT decision makers from various countries reports that 43 percent of current cloud users reported a security incident in the past 12 months (Trend Micro, 2011). Though the economic impact of a cloud security breach hasn't been easy to measure, there is scattered evidence to show the adverse effects of these breaches. Epsilon, a cloud based email service provider reported a breach in 2011 that affected approximately 75 client companies, exposing nearly 250 million customer emails. The cost of this breach was estimated to be between $3 – 4 billion (Privacy Rights Clearinghouse, 2011).

Research has shown that events of security breaches and their announcements have had significant and adverse impact on the market value of the firms involved. There is limited research on the impact of cloud computing announcements, specifically related to security and the consequences of a cloud security breach, on a company's performance in terms of sales, revenue and profitability. Since enterprises have already begun taking advantage of cloud services, the paper examines how announcements about security or privacy breach impact these firms.

Research Model

Since many companies use cloud services expecting reduction in costs and increase in business agility, it is important to measure and identify if such announcements on cloud computing really impact the market value of the firms (Fogarty, 2010; Pemmaraju, 2010). Research has shown that cloud computing announcements do have a significant impact on the stock prices of the companies involved (Parameswaran et al., 2011). In order to measure the impact of such announcements, internal measures such as return on investment or internal rate of return are difficult to apply to financial benefits obtained on IT investments, as there is very little information available about the changes to cash flows due to an

announcement (Dehning and Richardson, 2002). Since there are multiple factors influencing the cloud computing services, we employ an external measure to find the impact of these announcements. Since the time frame within which the announcements may affect the respective firms may vary, the stock price would show the impact more appropriately since it takes future costs and benefits into account (Agrawal et al., 2006). It is also independent of the likelihood of occurrence of the event. Thus, stock response could be a reliable and suitable indication of the effect of the announcements, which can be measured using event study (Dos Santos et al., 1993; Im et al., 2001). These announcements, which are related to cloud security, may have immediate or delayed impact. We therefore examine whether cloud computing security announcements affect the stock prices of various firms through three hypotheses.

Hypotheses Development

Researchers have widely studied the impact of security breach on market valuations of companies that suffer the breach (See For example, Acquisiti et al., 2006; Campbell et al., 2003; Cavusoglu et al., 2004; Ettredge and Richardson 2003;Garg et al. 2003b;Goel and Shawky, 2009; Telang and Wattal, 2006; Yayla and Hu, 2005). Garg et al. (2003a) estimate that, on average, breaches could lower annual sales of companies by 0.5 to 1 percent. A Ponemon study estimates that companies suffering from data breaches paid £47 per compromised record in 2007 and the average cost per reporting incident for the company is around £1.4m (Poneman, 2008). Extant studies have shown a significant negative impact due to information security breach (e.g., Ettredge and Richardson 2003; Garg et al. 2003a; Cavusoglu et al. 2004). Besides loss in stock value, there are long term costs associated with a security breach such as loss of trust, loss of business, legal actions and negative reputation (Cavusoglu et al., 2004; Tsiakis and Stephanides, 2005). Thus, we expect negative abnormal returns for cloud security breach announcements. Hence we hypothesize that:

H1a: *Cloud security breach announcements will have negative impact in market valuation of the involved companies*

Companies can plan initiatives in improvements in security practices after assessing their posture (Gupta et al, 2008; Tanna et al, 2005) and causes of the breach. Several studies have reported the reputational capital effect on stock performance of companies (Gregory, 1998; Knight and Pretty, 1999). Customers and stakeholders gain confidence about the company when announcements about a corrective action are made. These announcements help in restoring and uplifting the image that was damaged due to a crisis (Sellnow *et al.*, 1998). The crisis response to a cloud security breach incident can take the form of positive announcements regarding the company's security initiatives to further strengthen the overall security posture. After a security breach, positive security announcements such as partnership with a security services partner, or strengthening of authentication for customers (Gupta et al, 2004) or change

in security policies could be most effective in countering the negative publicity from the breach. These announcements that signify security counter measures or improvements can appease the negative impact of security breaches on the market value of the involved firms (Gupta, 2011). Thus, we expect positive abnormal returns for cloud security countermeasures announcements. Hence, we hypothesize that:

H1b: *Cloud computing security countermeasures announcements will have positive impact in market valuation of the involved companies.*

Event studies can reveal the impact of any event on the stock price of a firm. An investor's perception about a company's profitability and efficiency results in abnormal changes in the stock price. Customers shifting to competitors for same products or services usually accounts for a change in profitability. Adverse announcements like a cloud security breach have potential to affect the stock prices of other companies in the industry. Studies have shown certain events can cause competitors' stock prices to change. For example, Lang and Stulz (1992) show that at the time of the bankruptcy announcement, stock price of the bankrupt firm's competitors decreases by 1%, and the decline is statistically significant. Eckel et al. (1997) also showed a statistically and economically significant impact on competitors' market value due to airline privatization announcement. Research from Gupta et al. (2011) showed that stock prices of competitor companies in the financial sector tend to react in the same way as companies that have had an information security breach. Consequently, we expect a negative abnormal return for the competitors of the companies involved in a cloud security breach. Hence, we hypothesize that:

H2a: *Cloud security breach announcements will negatively impact market valuation of competitors of cloud companies involved*

It has been shown that companies prefer to keep their information related to breaches secret especially from competitors (Gordon and Loeb, 2001), to prevent reputation loss. However, in case such an event is known to public, by the same rationale companies would want to reveal their countermeasures and desire that the competitors would observe it. From a competitors' perspective such countermeasures may have a positive impact, more likely of the same sector or industry, since such countermeasures also reinstate the reputation of that particular industry or technology. Research from Gupta et al. (2011) also showed that competitors do benefit from positive security announcements from the companies that had a breach, across industries, firm types and years. Thus, we expect a positive abnormal return for the competitors of the companies involved in a cloud security countermeasure announcement too. Hence we hypothesize that:

H2b: *Cloud security countermeasures announcements will positively impact market valuation of competitors of cloud companies involved*

Cloud computing is more beneficial to SMBs, as there is no need to invest in new infrastructure, software licenses and staff training. With Cloud computing, small and medium-sized businesses can completely outsource their datacenter infrastructure while large companies that need huge load capacities can do without building large and expensive datacenters internally. (Dawoud, Takouna and Meinel, 2010). Since using Cloud computing can keep the IT budget to a bare minimum it is ideally suited for e-commerce entrepreneurs and for individuals seeking a quick solution for startups (Ramgovind, Eloff and Smith,2010). Studies have shown that large companies take advantage of cloud services only for some of their key IT elements (Molony and Kirchheime, 2011) when compared to SMBs whose profitability is entirely dependent on the cost savings and robustness provided by using the cloud services. A survey by Cisco states that SMBs are driving public cloud adoption when compared to large enterprises. The study reveals that half of the SMBs will spend at least one third of their IT budgets on Cloud computing services by 2013 (Taylor, Christensen, Young, Kumar and Macaulay, 2011). Thus, a security breach involving SMBs would convey more negative perception to investors when compared to large companies who are not entirely dependent on the cloud services for their profitability. Consequently, we expect cloud security breaches to impact SMBs more than large companies. Thus, we hypothesize:

H3: *Cloud security breach announcements would have affect small companies more when compared to large companies.*

RESEARCH METHODOLOGY

In this section, we describe how we collected and coded the cloud security announcements. We also provide a background on the event study methodology and calculation of abnormal returns using this methodology.

Data Collection

In this research, we collected 223 cloud computing announcements related to Information security. We used cloutage.org, a leading source of cloud security breaches, to collect announcements on cloud computing information security. We also used keyword search to collect more announcements on cloud computing information security. The keywords we used for the search to collect cloud security breach announcements include “cloud security breach” OR “cloud security announcements” OR “cloud security news” OR “cloud security breach” OR “cloud security data loss”. Some examples of cloud security breaches include:

“Apple App Store Suffers Hack Attack” (7/6/2010)

“Google password system was target of Chinese hackers” (4/10/2010)

“Salesforce.com crashes again” (1/31/2006)

In order to collect cloud security countermeasures news announcements, we used keywords including “cloud security technology” OR “cloud security fix” OR “cloud security investment” OR “cloud security improvement”. Some examples of cloud security countermeasures news include:

"Microsoft fixes bug in Windows Live file-sharing service" (12/10/2007)
"With encryption breakthrough IBM boost cloud computing" (7/5/2009)
"Amazon cloud-based database gains high-availability feature" (5/18/2010)

The announcements were also collected from press releases of the companies and popular news websites that release cloud computing news. The time period for data collection is four years – 2006 to 2010. We obtained historical stock price information for companies making the announcements from the Center for Research in Security Prices (CRSP) at the University of Chicago. CRSP contains price information of stocks listed in the New York Stock Exchange (NYSE), American Stock Exchange (AMEX), and NASDAQ (Andrade, et al., 2001). We also recorded the number of employees for each company involved in these cloud security announcements from finance.yahoo.com. We have classified companies with employee strength less than 5000 as small and medium businesses and companies with employee strength more than 5000 as large companies. Out of the 223 cloud computing announcements related to information security, there are 37 distinct companies that were involved in these announcements, 32 of which are publicly traded in the US market. The announcements that involved the 5 companies that are not publicly traded involved another company that is publicly traded. We also collected stock price information of 3 publicly traded competitors of each company involved in cloud security announcements. Competitor companies were identified using the "Hoovers" database as the source. In this analysis, the date of announcement has been used as the date to perform competitor analysis.

Hypothesis	Number of announcements	Data Description
H1a	188	Includes all publicly traded companies involved in a cloud security breach
H1b	35	Includes the publicly traded companies involved in a cloud security countermeasures news
H2a	188	Includes the competitors of the companies involved in a cloud security breach
H2b	35	Includes the competitors of the companies involved in a cloud security countermeasures news
H3	188	Employee strength < 5000 – Small and Medium businesses Employee Strength> 5000 – Large companies

Table 1: Data definition scheme

Event Study Methodology

Because of its popularity and relevance to IS research, Event Study has gained tremendous attention and traction, and such studies are becoming common in IS literature (Peak et al, 2002; Aggrawal et al, 2006; Hayes et al, 2001; Ranganathan and Brown, 2006; Dos Santos et al., 1993; Im et al, 2001; Koh and Venkatraman, 1991; Roztocki and Weistroffer, 2006; Agrawal et al, 2006; Cavusoglu et al., 2004;

Campbell et al., 2003, Gupta and Sharman, 2010; Song et al, 2007) amongst others. In our research, the Event Study methodology has been used to measure the firm's performance. We used market performance measures like stock prices in our study instead of accounting performance measures because the market measures take into account publicly available information to predict the cash flows and profits to establish the value of a firm. On the other hand, accounting performance measures are used only when the benefits of an event and the exact time period in which the benefits can be obtained are defined accurately (Agrawal et al, 2006; Dehning and Richardson, 2002; Beasley, Bradford and Dehning, 2009). Our paper studies whether the market adjustment made to the value of firms due to cloud computing security announcements are witnessed immediately in the form of changes in the stock market prices of the firms. Immediate changes would tell us that the market does react to the cloud computing security announcements (Agrawal et al., 2006). We also assess how an announcement of cloud security breaches and countermeasures changes the stock prices of the competitors of the companies involved.

Abnormal Returns

In our research, abnormal stock returns serve as the metric of the economic impact of cloud security breach and countermeasures announcements. In an event study, abnormal returns are calculated for an event window. The most important choice in an event study is the choice of the length of the event window (Agrawal et al., 2006, McWilliams et al., 1997). Based on prior event studies in the field of information systems, we chose event windows of (-1,1) (-1,2) (-1,3) (-1,4) and (0,1) (0,2) (0,3) (0,4) in addition to taking the actual date of announcement or the zeroth day.

We used the market adjusted returns model for the computation of abnormal returns. To compute the abnormal returns, we used the Eventus software package. Given an event window and the model for abnormal returns calculation, the Eventus software computes the abnormal returns for firms for that window by interfacing SAS and the CRSP database (Agrawal et al., 2006).

Based on the Market adjusted model, the abnormal returns for a firm *i* on day *t* is,

$$A_{it} = R_{it} - R_{mt}$$

Where, R_{it} is the return of stock for firm *i* on day *t*

R_{mt} is the CSRP value weighted market return on the same day

Since we are looking at *N* firms, we need to aggregate the abnormal returns for each day for the period *t*; therefore, we formulate Mean Abnormal Return (MAR_t),

$$MAR_t = \sum_{i=1}^{N} AR_{it}$$

Cumulative Abnormal Return (CAR) is used to measure the change in firm value. The CAR for the cloud computing announcements for the firm *i* for the period *t1* to *t2*is given by

$$\mathrm{CAR_i}(t1, t2) = \sum_{t=t1}^{t=t2} \mathrm{A_{it}}$$

In our research, since we are looking at the CAR for many firms, we need to compute the Average Cumulative Abnormal Return (ACAR). For an event window *T*, the ACAR for *N* firms is given by,

$$\mathrm{ACAR_i}(t1, t2) = 1/\mathrm{n} \sum_{t=1}^{n} \mathrm{A_{it}}$$

Then we use Patell Z test statistic (a standardized parameteric test) to check if the ACAR is significantly (statistically) different from zero. If significance is found in this test, we can say that the cloud computing security announcements made an impact on the stock market. The magnitude of the impact can also be inferred based on the level of significance (Agrawal et al., 2006; Beasley et al, 2009; Goel and Shawky, 2009; Mcwilliams et al., 1997).

RESULTS

We investigated nine event windows for evaluating impact of cloud computing security announcements on the companies involved and on different stakeholder companies such as competitors. We had nine event windows for each hypothesis, and in this section, we only present the ones that show any significance. For each hypothesis, we have omitted event windows that report inconclusive results. A summary of results for all the hypotheses is shown below:

Hypothesis	Description	Hypothesized effect	Support	Results
H1a	*Cloud security breach announcements will have negative impact in market valuation of the involved companies*	-	Supported.	Significant -ve MAR on zeroth day (see Table 9).
H1b	*Cloud security countermeasures announcements will have positive impact in market valuation of the involved companies.*	+	Not supported but we get counter-intuitive results.	Significant –ve CARs on the window (0,-1) (see Table 4)
H2a	*Cloud security breach announcements will negatively impact market valuation of competitors of Cloud companies involved*	-	Supported	Significant –ve CARs on the window (-1,0) (-1,3) (see Table 5)

H2b	*Cloud security countermeasures announcements will positively impact market valuation of competitors of Cloud companies involved*	+	Not supported but we get counter-intuitive results. -ve abnormal returns.	Significant –ve CARs on the window (0,1) (see Table 6)
H3	*Cloud security breach announcements would have affect small companies more when compared to large companies.*	Small companies should have lesser returns than large companies	Not supported but we get counter-intuitive results.	Large companies have –ve impact and smaller ones have +ve impact (see Tables 7,8 and 9)

Table 2: Window based results of all cloud computing security announcements

Window	ACAR	Positive:Negative	Patell Z	Generalized Sign Z
(-1,0)	-0.03%	86:97	-0.529	-0.235
(0,+1)	-0.29%	79:104	-1.619$	-1.271
(0, +2)	0.05%	86:97	-0.397	-0.235
(0, +3)	0.09%	81:102	-0.233	-0.975

Table 3: Window based results of cloud security breach announcements

Table 3 shows the Average Cumulative abnormal returns for the companies involved in the cloud security breach announcements from 2006 to 2010. The windows do not show any significant abnormal returns.

Window	ACAR	Positive:Negative	Patell Z	Generalized Sign Z
(-1,0)	-0.54%	10:21<	-0.788	-1.705*
(0,+1)	-0.33%	11:20(	-0.706	-1.345$
(0, +2)	-0.78%	11:20(	-0.673	-1.345$
(0, +3)	-0.43%	14:17	0.574	-0.266

Table 4: Window based results of cloud security countermeasures announcements

Table 4 shows the Average Cumulative abnormal returns for the companies involved in the cloud security countermeasures announcements from 2006 to 2010. The result is negative for windows (-1, 0) at 5% level of significance with ACAR as -0.54% for the generalized test. The windows (0, +1) and (0, +2) show negative abnormal returns with 10% level of significance. This shows that there was a negative impact of a cloud security countermeasures announcement on the respective companies.

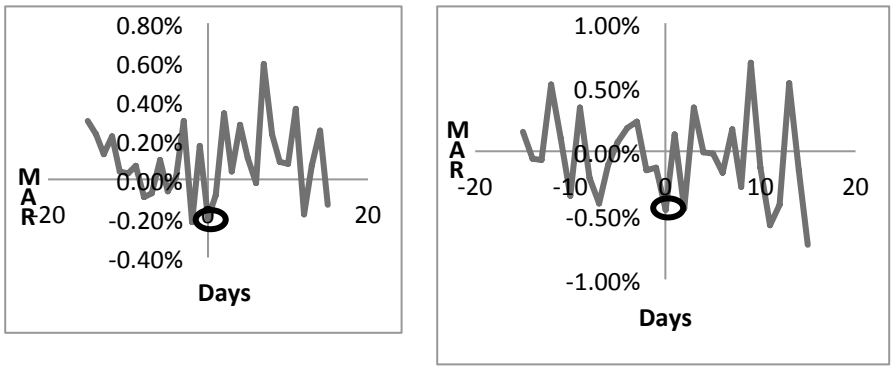

Figure 1: CARS of Cloud security breach and countermeasures news announcements

Figure 1 shows daily mean abnormal returns for 15 days before and after cloud security breach incidents and cloud security countermeasures announcements respectively. In both the cases, we see a spike on the day of the announcement.

Window	ACAR	Positive:Negative	Patell Z	Generalized Sign Z
(-1,+3)	-0.17%	165:232<	-1.220	-1.931*
(-1,+2)	-0.07%	171:226(	-0.785	-1.327$
(-1,0)	-0.09%	167:230<	-1.051	-1.730*
(0,+1)	-0.16%	175:222	-0.792	-0.925
(0, +2)	-0.13%	186:211	-0.895	0.182
(0, +3)	-0.22%	174:223	-1.354$	-1.025

Table 5: Window based results of competitors of companies with breach announcements

Table 5 shows the Average Cumulative abnormal returns for the competitors of companies involved in a cloud security breach announcement from 2006 to 2010. The result is negative for windows (-1, +3) (-1, 0) at 5% level of significance with ACAR as -0.17%, -0.09% respectively for the generalized test. The windows (0, +3) and (-1, +2) show negative abnormal returns with 10% level of significance. This shows that there was a negative impact of a negative cloud security announcement on the competitors of the respective companies.

Window	ACAR	Positive:Negative	Patell Z	Generalized Sign Z
(-1,+3)	-0.53%	41:62	-1.045	-1.391$
(-1,+2)	-0.70%	42:61	-1.611$	-1.194
(-1,0)	-0.25%	48:55	-0.686	-0.009
(0,+1)	-0.32%	36:67	-0.823	-2.379**
(0, +2)	-0.51%	42:61	-1.252	-1.194
(0, +3)	-0.34%	47:56	-0.641	-0.206
(0,+5)	-0.25%	56:47	0.069	1.572$

Table 6: Window based results of competitors of companies with countermeasure announcement

Table 6 shows the Average Cumulative abnormal returns for the competitors of companies involved in the cloud security countermeasures announcements from 2006 to 2010. The result is negative for window (0, +1) at 1% level of significance with ACAR as -0.32% for the generalized test. The windows (0, +5) (-1, +2) and (-1, +3) show negative abnormal returns with 10% level of significance. This shows that there was a negative impact of cloud security countermeasures announcement on the competitors of the respective companies.

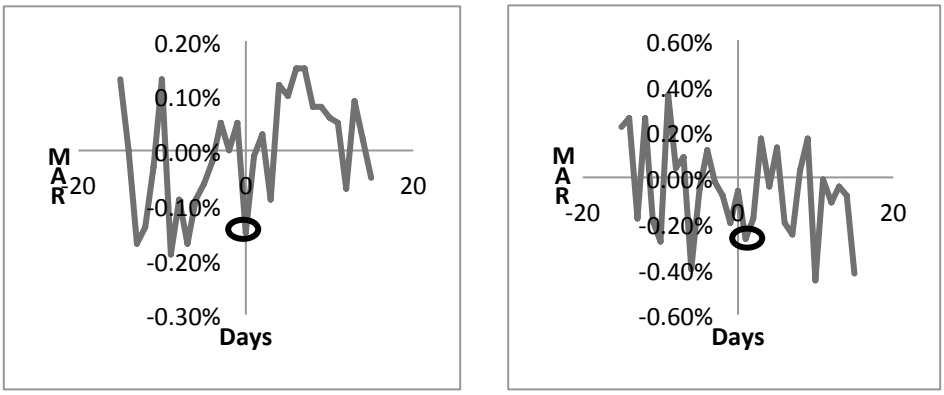

Figure 2: CARS of competitors of companies involved in cloud security breach and countermeasures news announcements

Figure 2 shows daily mean abnormal returns of competitors for 15 days before and after cloud security breach incidents and cloud security countermeasures announcements respectively. We see a spike on the day of the announcement for the competitors of cloud security breach and a spike 1 day after the announcement for competitors of cloud security countermeasures news.

Window	ACAR	Positive:Negative	Patell Z	Generalized Sign Z
(-1,+4)	1.90%	41:24	2.297*	2.288*
(-1,+3)	1.40%	41:24	1.849*	2.288*
(-1,+2)	1.22%	39:26	1.821*	1.792*
(-1,1)	1.40%	37:28	0.836	1.296$
(-1,0)	1.90%	36:29	1.112	1.047
(0,+1)	-0.02%	29:36	-0.047	-0.689
(0, +2)	0.69%	31:34	1.227	-0.193
(0, +3)	0.87%	35:30	1.308$	0.799
(0,+4)	1.37%	40:25	1.837*	2.040*
(0,+5)	1.59%	43:22	1.958*	2.784**

Table 7: Window based results of cloud security breach announcements of small and medium business companies

Table 7 shows the Average Cumulative abnormal returns for small companies involved in a Cloud security breach announcement from 2006 to 2010. The result is positive for window (0, +5) at 1% level of significance with ACAR as 1.59% for the generalized test. The windows (-1, +4) (-1, +2) (0,+4) and (-1, +3) show positive abnormal returns with 5% level of significance. This shows that there was a positive impact of a cloud security breach on small and medium business companies.

Window	ACAR	Positive:Negative	Patell Z	Generalized Sign Z
(-1,+4)	-0.19%	54:70	-0.727	-0.836
(-1,+3)	-0.32%	52:72	-1.087	-1.196
(-1,+2)	-0.24%	57:67	-1.009	-0.296
(-1,+1)	-0.36%	56:68	-1.307$	-0.476
(-1,0)	-0.31%	53:71	-1.360$	-1.016
(0,+1)	-0.37%	54:70	-1.797*	-0.836
(0, +2)	-0.25%	59:65	-1.325$	0.063
(0, +3)	-0.33%	48:76	-1.354$	-1.915*
(0,+4)	-0.20%	50:74	-0.92	-1.555$
(0,+5)	-0.17%	54:70	-0.622	-0.836

Table 8: Window based results of cloud security breach announcements of large companies

Table 8 shows the Average Cumulative abnormal returns for the large companies involved in a cloud security breach announcement from 2006 to 2010. The windows (0, +1) and (0, +3) show negative abnormal returns with 5% level of significance on the Patell Z test and the generalized sign test respectively. This shows that there was a negative impact of a cloud security breach on large companies.

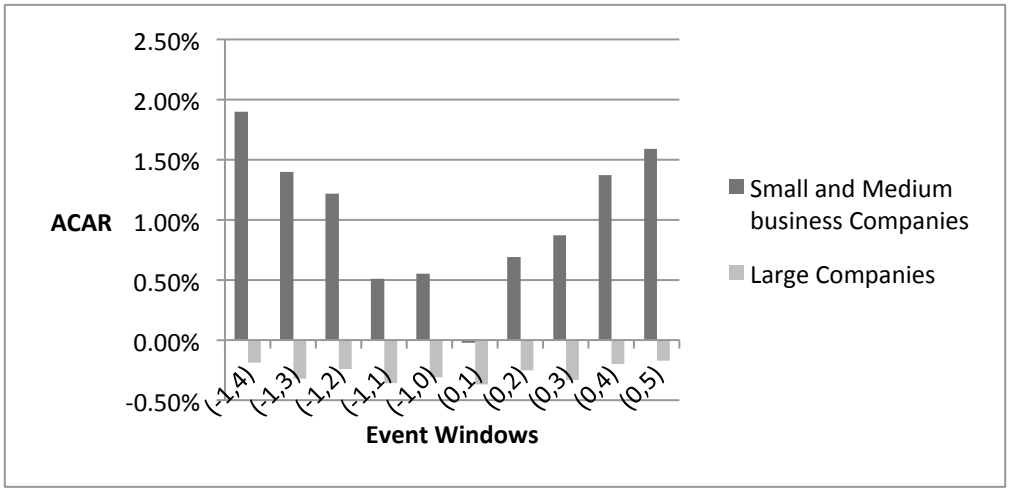

Figure 3: ACAR of Small companies versus Large companies

Figure 3 shows a comparison of Average cumulative abnormal returns of small and medium business companies versus large companies that have had a cloud security breach. It is clearly evident from the figure that small companies have benefited from a cloud security breach whereas large companies have had a negative impact.

Hypothesis	ACAR	Positive:Negative	Patell Z	Generalized Sign Z
H1a	-0.20%	82:101	-1.742*	-0.827
H1b	-0.46%	11:20(	-0.766	-1.345$
H2a	-0.15%	173:224<	-1.468$	-1.126
H2b	-0.06%	48:55	0.085	-0.009
H3 (Small companies)	0.02%	31:34	0.059	-0.193
H3 (Large companies)	-0.32%	53:71	-2.201*	-1.016

Table 9: Mean abnormal returns on the day of announcement for all hypotheses

Table 9 shows the Market Adjusted mean abnormal returns on the day of announcement for all the companies under the three stated hypotheses. The hypothesis H1a is supported with a 5% level of significance for the Patell Z test. The hypothesis H2a is supported with a 10% level of significance for the Patell z test. The hypotheses surrounding the cloud security countermeasures news and the competitors of companies involved in such news are not supported. Instead we get counter-intuitive results. This is also the case with the hypothesis surrounding the small and medium business companies versus large companies.

Cloud Security Breach versus Information Security Breach

In this section, we compare the impact of cloud security breaches on the firm valuation to that of information security breaches from research by Gupta (2011).

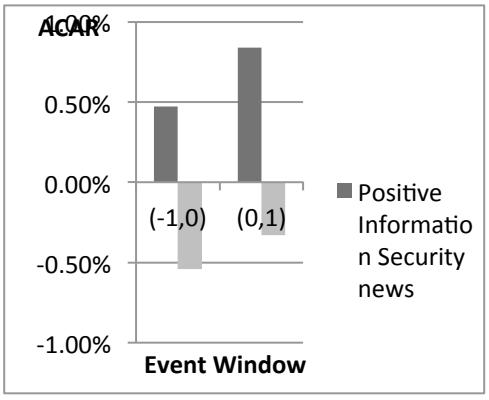

Figure 4: Cloud Security countermeasures versus Information Security countermeasures

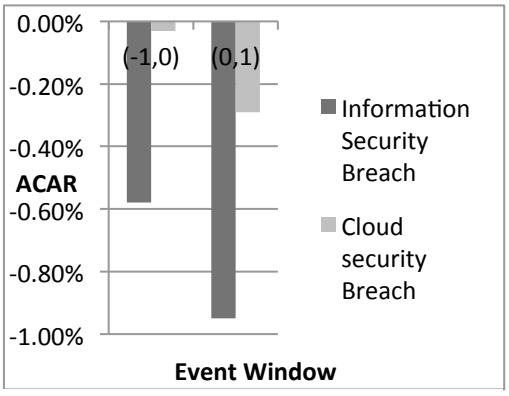

Figure 5: Cloud Security breach versus Information Security Breach

Gupta (2011) showed a significant negative impact on the companies involved in information security breaches. The research also shows significant positive abnormal returns for the companies involved in a cloud security countermeasure announcement. Figure 5 illustrates the comparison of ACARs of information security breaches versus cloud security breaches. Cloud security breaches have had less impact when compared to the impact of information security breaches from research by Gupta (2011).

However, cloud security countermeasures news has had significant negative impact on the market valuation of the firms involved when compared to positive abnormal returns due to information security countermeasures announcements. Figure 4 illustrates the comparison of ACAR's of information security countermeasures news versus cloud security countermeasures news.

FRAMING EFFECTS OF CLOUD SECURITY ANNOUNCEMENTS

Given the significant impact of cloud security breaches on firm valuation, we investigated whether the magnitude of impact differs with the way these announcements are framed. We examine the impact of the use of certain frames in cloud security breach announcements on stock price. Such a study can guide PR personnel to ensure that cloud security breach announcements are made using optional frames to maximize the positive impact on the stock market. Framing effect is a phenomenon where a communicator emphasizes or uses certain factors to influence opinions and judgments of readers (Druckman, 2001).

Communications studies have widely established that frames in communication (images, words, phrases, etc.) impact the way the information is presented and received. Frames (or keywords) are important to project certain facts or values as important so as to make them salient and thus important to the users (Josyln, 2003). Cooper (2002) asserts that framing of a message is critical in defining problems, attributions and solutions.

We used 'Textexture' to find out the most influential frames in our cloud security breach announcement articles. Textexture is an online tool developed by Dmitry Paranyushkin from Nodus Labs to read polysingularity of text. Polysingularity is a condition where multiple solutions are possible but only some can be actualized at a particular moment in time (Paranyushkin, 2012). Framing of a cloud security announcement is based on the choice of the words by the author. But some words more often align well together that form broad themes that dominate these cloud security announcements. This is known as polysingularity of a cloud security announcement. Textexture scans the text for patterns of words that occur close to each other and within attention span gaps (Paranyushkin, 2012). It removes words like "the", "is", "are" and constructs a graph where the nodes represent the words and the edges represent the co-occurrence of words. Texture uses 3 graph processing algorithms based on social network theories to read polysingularity of text. More information on the algorithms can be found in the Textexture website.

We merged the 188 cloud security breach announcements and used it as input to the Textexture tool. The following was obtained as output from the Textexture tool: 1) a list of four influential keywords in the text 2) a list of four arrays that represent the most influential context in the text 3) a network graph for cloud security announcements. The four most influential keywords in the cloud security announcements were service, user, company and problem. Figure 6 shows the network graph generated by Textexture based on the analysis of all the cloud security announcements.

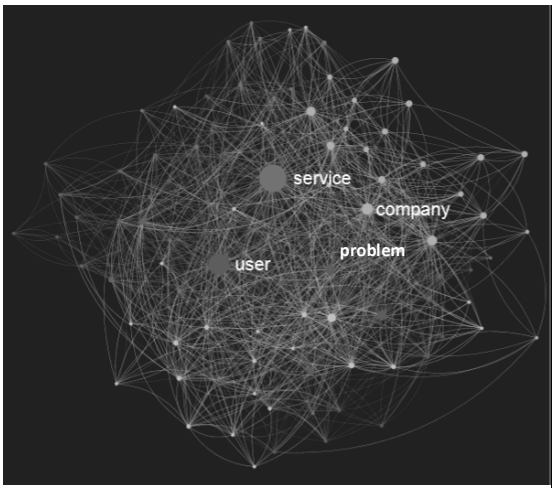

Figure 6: Network graph for 188 cloud security announcements

Table 10 lists the four most influential themes generated by Textexture based on the analysis of all the cloud security announcements.

service	control	services	support
problem	outage	delay	report
company	customer	host	users
app	server	online	data

Table 10: Top 4 most influential contexts

Based on the keywords in the top 4 most influential contexts generated by textexture, we identified the 4 broad themes that dominate the framing of cloud security announcements. Each context was identified as belonging to the following four themes. 1) business and management, 2) security 3) stakeholders and 4) technology.

Context	**Themes**
service control services support	Business and management
problem outage delay report	Security
company customer host users	Stakeholders
app server online data	Technology

Table 11: Mapping contexts to themes

Table 11 shows the mapping of the influential contexts to the corresponding themes. We used these themes to categorize the keywords we obtained from frequency analysis of cloud security announcements, which will be discussed in the following section. Then we performed a theme-impact analysis to determine the themes that dominate the best performing announcements. Figure 7 illustrates the steps involved in analyzing the framing effects of cloud security announcement.

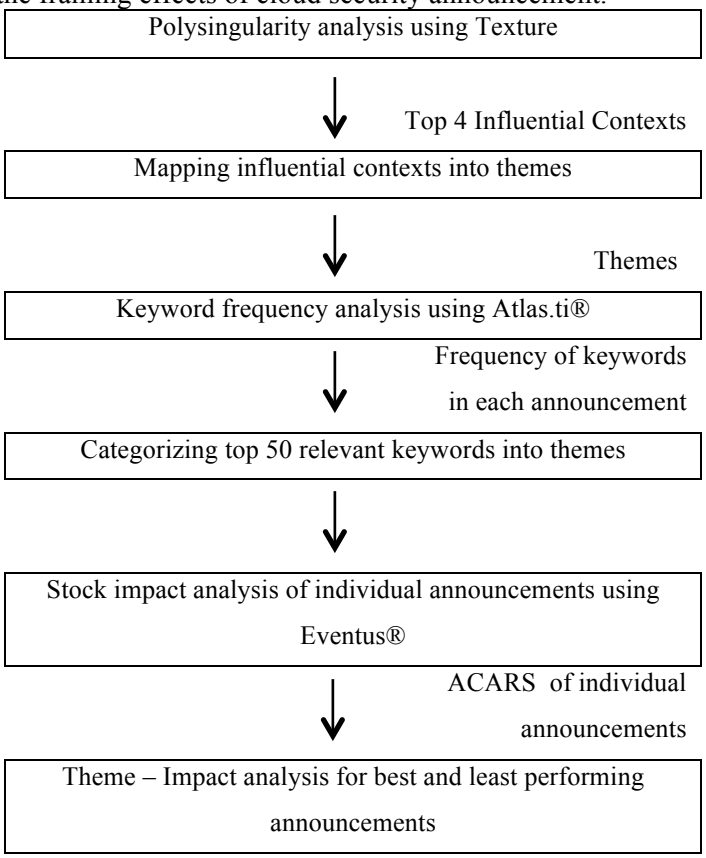

Figure 7: Steps in analyzing the framing effects

In our analysis, we used keywords as proxies for the frames. We analyzed the 188 cloud security breach announcements made by the firms for keyword frequency. We individually collected the impact on stock prices due to each announcement using event study methodology. Eventus® software was used to run 193 outputs with one for each event for the consumer and the provider. These results from the event study were subsequently used for further analysis using content analyses. We used Atlas.ti ® (version 6.0) for content analysis. We obtained 56,214 words with 6226 unique keywords. We removed the keywords that occurred less than 200 times. We then removed the common words like "the", "an", "are" etc. to arrive at 50 keywords which were categorized into four broad themes identified using polysingularity analysis: 1) business and management, 2) stakeholders 3) technology and 4) Security.

Keywords for each theme are as follows: Business and Management (service, services, control, support, companies, performance, enterprise, infrastructure, enterprises); Stakeholders (users, customers, engineers, company, customer, people); Technology (data, storage, apps, software, online, update, web, applications, files, sites, information, updates, server, network, hosted, app, application, servers); and Security (delays, outages, connectivity, availability, account, accounts, report, backup).

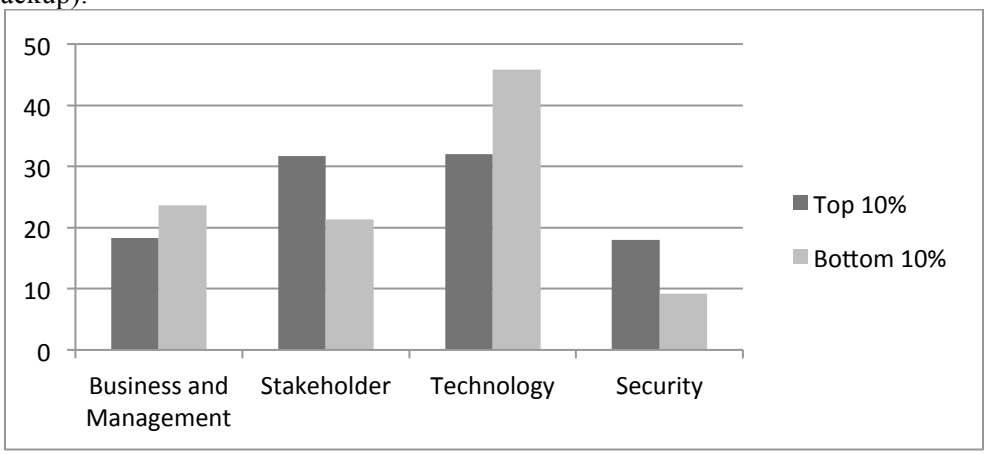

Figure 8: Content analysis: Top 10% vs Bottom 10% performing announcements

The announcements were sorted based on their impact on the stock price of the company involved in the announcement. Figure 8 shows the keywords used in the top 10% and bottom 10% performing announcements. The top 10% used more security-related and stakeholder related keywords, while the last 10% used the more business\management and technology keywords.

These observations were confirmed by the results of test of difference in proportion at 5% level of significance. From our results, we can infer that investors foresee future profitability of the company when stakeholder and security related keywords are used. Our content analysis can be used to cue managers on the keywords that responded more positively when a cloud security breach announcement is made. The study also sheds light on the type of keywords that must be avoided while framing cloud security breach announcements.

IMPLICATIONS AND CONCLUSION

Research shows that information security events, in general, have had significant impact on the stock value of the firms and their competitors (Gupta, 2011; Goel and Shawky, 2009). Our research shows that information security breaches related to cloud computing has significant negative impact on the stock value of the firms on the day of announcement. When compared to impact of information security breaches, cloud security breaches have relatively a less negative impact. This study

also reveals that the competitors of the companies involved in a cloud security breach experience a significant negative impact on the firm valuation. Contrary to research on the effect of information security countermeasures news on the companies and competitors (Gupta, 2011), our research shows that cloud security countermeasures news has significant negative impact on the firm valuation involving companies. Contrary to our hypothesis, large companies seem to be affected by a cloud security breach whereas small and medium business companies seem to benefit from a cloud security breach.

In its current stage of evolution and adoption, cloud computing has more advantages than disadvantages. The advantages are for both the providers and adopters. While adopters are looking to cloud to reduce capital costs, divest infrastructure management and leverage on-demand provisioning of services to manage "cloud bursts", they are equally concerned about potential security risks of the solutions. The last few years have seen security concerns as a major hindrance to both innovation of cloud based services and in adoption of those services. The research presented in the paper is useful for both sides to understand the value of security lapses on investors' perception. This, in turn, also impacts the overall confidence that the customers and other stakeholders have on both providers and adopters. This research also provides unique insights into differences between other data/security breaches and cloud computing security breaches and their impact on competitors of affected companies. The companies usually assume a cloud computing security incident to be yet another data breach, but characteristics of cloud computing yield different response, as our research shows. An interesting implication from the results is that competitors show contagion effect for negative announcements, but the countermeasures announcements show opposite results. The implications are serious for cloud computing providers, for the results show a strong contagion effect for security breaches. Those companies should work together in information sharing and developing better and more effective strategies and solutions for thwarting existing and potential risks. These collaborative initiatives help not only individual companies, but all companies involved in the similar business of offering cloud computing services. Cloud computing companies can benefit from the study in formulating their own crisis response strategies for mitigating the negative impact on their market valuation due to security breaches (Gupta, 2011).

While some customers believe that cloud computing heralds the possibility of a new generation of transformative services, others believe that it is just re-packaging of extant technologies. In either case, security concerns have always been there; it's only that with recent increase in adoption, the security issues have taken center stage in the decision-making process about cloud adoption. The investors in the companies that offer and adopt cloud computing are excited about the cost savings and innovative services. In light of the fact that security has been a major issue in cloud adoption, the research presented in the paper provides insights into how investors perceive announced security issues in cloud computing. Regulators in certain sectors, including financial, have warned/advised banks to ensure strong and effective controls to reduce risk and to ensure safe computing environment (Borak, 2012). Under stricter

supervision and scrutiny, cloud service providers have never been more cautious in implementing and promoting security of the data and processes of the cloud adopters.

The Gartner Hype cycle for 2011 has positioned cloud security at the Peak of Inflated Expectations, a phase that is characterized by huge publicity eventually generating over-enthusiasm and unrealistic expectations. Any announcement regarding a firm's cloud security breach or a cloud security countermeasures announcement would be subject to interest of the customers or the key stakeholders of the company. As the adoption of cloud computing has started increasing (Molony and Kirchheime, 2011), cloud security has emerged as a top area of concern over the years (Symantec, 2011).The issue of cloud security has reached a point where investors have started to take cloud security announcements more seriously by perceiving a security breach as a negative information about the company.

LIMITATIONS AND FUTURE STUDY

We have analyzed the market impact of cloud security breaches and countermeasures news on firm valuation of the companies involved. However, there are a few limitations to our study. Firstly, our study is limited to publicly traded companies listed in the New York Stock Exchange (NYSE), American Stock Exchange (AMEX), and NASDAQ whose price information is listed in the CRSP database. Secondly, adverse events like a cloud security breach could be subjected to confounding effects of other adverse events in the same time period. In future work, we would explore the confounding effects of other events on cloud security breaches and countermeasures news. Thirdly, since we have collected data from press releases of the companies and popular news websites that release cloud computing news, we have not accounted for any leakages in the news prior to the release. Finally, as is the case with any other event study, our research makes the assumption of market efficiency and that news media announcement about a firm will be reflected immediately in the stock price. Since we have analyzed cloud security breaches as a whole, future research can be done on the impact of the types of cloud security breaches like data-losses, hacks and outages on the market valuation of the firms. Research can also analyze the stock impact of the different types of countermeasures. We hope that more research is done in this area of cloud security breaches and investigate how important is cloud security in the adoption of cloud computing.

REFERENCES

Acquisti, A., Friedman, A., &Telang, R. (2006). IS THERE A COST TO PRIVACY BREACHES? AN EVENT STUDY. Fifth Workshop on the Economics of Information Security (pp. 1-20). Citeseer. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.73.2942&rep=rep1&type=pdf

Aggarwal, N., Dai, Q. and Walden, E.A. (2006). Do Markets Prefer Open or Proprietary Standards for XML Standardization?.International Journal of Electronic Commerc. 11(1) 117-136.

Agrawal, M., Kishore, R. and Rao, H.R. (2006). Market reactions to e-business outsourcing announcements: An event study. Information & Management, 43(7), 861-873.

Andrade, G. Mitchell, M. and Stafford, E. (2001) New Evidence and Perspectives on Mergers, The Journal of Economic Perspectives, 15(2), 103-120

Beasley, M. Bradford, M. and Dehning, B. (2009) The value impact of strategic intent on firms engaged in information systems outsourcing, International Journal of Accounting Information Systems, 10, 2, 79-96

Borak, D. (2012). Regulators Warn Banks of Risk from Cloud Services, American Banker: Regulation and Reform. http://www.americanbanker.com/issues/177_132/regulators-warn-banks-of-risk-from-cloud-services-1050787-1.html

Brodkin, J. (2008). Gartner: Seven cloud-computing security risks. *Infoworld*, 1-3.

Campbell, K., Gordon, L.A., Loeb, M.P., and Zhou, L. (2003). "The economic cost of publicly announced information security breaches: Empirical evidence from the stock market," Journal of Computer Security, 11, 3 (March 2003), 431–448.

Carroll, C. E., & McCombs, M. (2003). Agenda-setting Effects of Business News on the Public's Images and Opinions about Major Corporations. Corporate Reputation Review, 6(1), 36-46. Henry Stewart Publications. doi:10.1057/palgrave.crr.1540188

Catteddu, D. and Hogben, G. (2009). "Cloud Computing: Benefits, Risks and Recommendations for Information Security", Nov 20, 2009, Retrieved from http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment

Cavusoglu, H., Mishra, B. and 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, Vol. 9, Number 1, 2004, pp. 69-104.

Che, J., Duan, Y., Zhang, T., & Fan, J. (2011). Study on the Security Models and Strategies of Cloud Computing. Procedia Engineering, 23, 586-593. doi:10.1016/j.proeng.2011.11.2551

Chen, C. C., &Meindl, J. R. (1991). The Construction of Leadership Images in the Popular Press: The Case of Donald Burr and People Express. Administrative Science Quarterly, 36(4), 521. Administrative Science Quarterly. doi:10.2307/2393273

Chen, Y., Paxson, V., & Katz, R. H. (2010). What's New About Cloud Computing Security? University of California Berkeley Report No UCBEECS20105 January (Vol. 20, pp. 2010–5). Electrical Engineering and Computer Sciences. Retrieved from http://www.eecs.berkeley.edu/Pubs/TechRpts/2010/EECS-2010-5.html

Cooper, A. H. (2002). Media framing and social movement mobilization: German peace protest against INF missiles, the Gulf War, and NATO peace enforcement in Bosnia. European Journal of Political Research, 41(1), 37-80.

Dawoud, W., Takouna, I., &Meinel, C. (2010). Infrastructure as a Service Security : Challenges and Solutions. Security, 1–8. IEEE. Retrieved from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5461732

Deephouse, D. L. (2000). Media Reputation as a Strategic Resource: An Integration of Mass Communication and Resource-Based Theories. Journal of Management, 26(6), 1091-1112. doi:10.1177/014920630002600602

Dehning B, and Richardson VJ. (2002). Returns on investments in information technology: a research synthesis. Journal of Information Systems 2002;16(1):7–30 [Spring]

Dos Santos, B.L., Peffers, K., and 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.

Druckman, J. N. (2001). The implications of framing effects for citizen competence. Political Behavior, *23*(3), 225-256.

Dutton, J. E., &Dukerich, J. M. (1991). KEEPING AN EYE ON THE MIRROR : IMAGE AND IDENTITY IN ORGANIZATIONAL ADAPTATION. Academy of Management Journal, 34(3), 517-554. JSTOR. doi:10.2307/256405

Eckel, C., Eckel, D., and Singal, V. (1997). "Privatization and efficiency: Industry effects of the sale of British Airways", Journal of Financial Economics, 43 (1997) 275-298

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

Fogarty, K. (2010, July 8). Cloud Computing: Today's Four Favorite Flavors, Explained. Retrieved from http://www.cio.com/article/598918/Cloud_Computing_Today_s_Four_Favorite_Flavors_Explained

Garg, A., Curtis, J. and Halper, H. (2003a). "The financial impact of IT security breaches: what do investors think?," Information Systems Security, Vol. 12, Number 1, 2003, pp. 22-33. 189

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

Goel, S. and Shawky, H.A. (2009) Estimating the market impact of security breach announcements on firm values, Information & Management, 46, 7, 404-410

Gordon, L. A., & Loeb, M. P. (2001). Using information security as a response to competitor analysis systems. *Communications of the ACM*, *44*(9), 70-75.

Gregory, J. R. (1998). "Does corporate reputation provide a cushion to companies facing market volatility? Some supportive evidence," Corporate Reputation Review, 1, 288 – 290

Gupta, M. and Sharman, R. (2010). "Impact of Web Portal Announcements on Market Valuations: An Event Study", International Journal of Web Portals, Volume 2, Issue 4, 2010.

Gupta, M., Banerjee, S., Agrawal, M. and Rao, H. R. (2008). "Security Analysis of Internet Technology Components Enabling Globally Distributed Workplaces – A framework". ACM Transactions on Internet Technology, November 2008 (volume 8, number 4)

Gupta, M., Rao, H. R. and S. Upadhyaya. (2004). "Electronic Banking and Information Assurance Issues: Survey and Synthesis". Journal of Organizational and End User Computing, Vol. 16, No. 3, pp. 1-21, July- September 2004

Gupta, M. (2011). Three essays on information technology security management in organizations. Ph.D. dissertation, State University of New York at Buffalo, United States -- New York. Retrieved January 4, 2012, from Dissertations & Theses @ SUNY Buffalo.(Publication No. AAT 3440288).

Hasan, R., & Yurcik, W. (2006). A statistical analysis of disclosed storage security breaches. Proceedings of the second ACM workshop on Storage security and survivability StorageSS 06 (p. 1). ACM Press. doi:10.1145/1179559.1179561

Hayes, D.C., Hunton, J.E. and Reck, J. L. (2001). "Market Reaction to ERP Implementation Announcements," Journal of Information Systems, 15, 1, 3-18.

Heiser, J., & Nicolett, M. (2008). Assessing the security risks of cloud computing. *Gartner Report*.

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. doi:10.1046/J.1098-1616.2003.026.x

Im, K.S., Dow, K.E. and Grover, V. (2001). "Research Report: A Reexamination of IT Investment and the Market Value of the Firm - An Event Study Methodology," Information Systems Research, 12, 1, 103-117.

Jensen, M., Schwenk, J., Gruschka, N., & Iacono, L. L. (2009). On Technical Security Issues in Cloud Computing. 2009 IEEE International Conference on Cloud Computing, 0(2009), 109-116. Ieee. doi:10.1109/CLOUD.2009.60

Joslyn, M. R. (2003). Framing the Lewinsky Affair: Third-Person Judgments by Scandal Frame. *Political Psychology*, *24*(4), 829-844

Kark, K. (2008). "Security breach management: planning and preparation." SearchSecurity.com, http://searchsecurity.techtarget.com/ tip/0, 289483,sid14_gci1314823,00.html

Knight, R. F. and Pretty, D. J. (1999). "Corporate catastrophes, stock returns, and trading volume," Corporate Reputation Review, 2, 363 – 381

Koh, J. and Venkatraman, N. (1991) "Joint venture formations and stock market reactions: an assessment in the information technology sector", Academy of Management Journal, Vol. 34 No. 4, pp. 869-92.

Lang, L. H. P and Stulz, R. M. (1992). "Contagion and competitive intra-industry effects of bankruptcy announcements - An empirical analysis", Journal of Financial Economics, 32 (1992) 45-60. North-Holland

Liginlal, D., Sim, I., &Khansa, L. (2009). How significant is human error as a cause of privacy breaches? An empirical study and a framework for error management. Computers Security, 28(3-4), 215-228. Elsevier Ltd. doi:10.1016/j.cose.2008.11.003

Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., &Ghalsasi, A. (2011). Cloud computing — The business perspective. Decision Support Systems, 51(1), 176-189. Elsevier B.V. doi:10.1016/j.dss.2010.12.006

Mather, T., Kumaraswamy, S., & Latif, S. (2009). *Cloud security and privacy: an enterprise perspective on risks and compliance*. O'Reilly Media, Incorporated.

McWilliams, A. and Siegel, D. (1997) Event studies in management research: theoretical and empirical issues, Academy of Management Journal 40, 626–657.

Mell. P (2011) "The NIST Definition of Cloud Computing (Draft), Recommendations of the National Institute of Standards and Technology", January 2011, Retrieved from http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf

Molony, D. and Kirchheime, E. (2011). What multinationals want: Opportunities in cloud computing Retrieved January 1, 2012, from http://www.cw.com/assets/content/pdfs/resource/ovum-cloud-wp.pdf

Parameswaran, S.,Venkatesan, S., Gupta, Manish., Sharman, Raj.and Rao, H. R., "Impact of Cloud Computing Announcements on Firm Valuation" (2011). AMCIS 2011 Proceedings - All Submissions. Retrieved from http://aisel.aisnet.org/amcis2011_submissions/291

Parameswaran, S., Venkatesan, S. and Gupta, M. (2012). "Do Cloud Security Announcements affect Firm Valuation?" Proceedings of Annual Symposium on Information Assurance and Secure Knowledge Management (ASIA & SKM' 12) June 5-6, 2012, Albany, N.Y.

Paranyushkin, D. (2012). Visualize any text as a network - Textexture. Retrieved November 18, 2012, from http://www.textexture.com/index.php.

Peak, D., Windsor, J. and Conover, J. (2002). "Risks and effects of IS/IT outsourcing: a securities market assessment," Journal of Information Technology Cases and Applications 4 (1), 2002, pp. 6–33.

Pemmaraju, K. (2010). "Cloud Leaders: Act Now", Sand Hill Group Report, March 24, 2010, Retrieved from http://www.sandhill.com/opinion/editorial.php?id=296

Poneman. (2008). “Ponemon evaluates cost of UK breaches,” Network Security Magazine, March 2008, Pp 2

Privacy Rights Clearinghouse. (2011).Data Breaches: A Year in Review. Retrieved from: https://www.privacyrights.org/top-data-breach-list-2011

Ramgovind, S., Eloff, M.M., and Smith, E.(2010). The management of security in Cloud computing Information Security for South Africa (ISSA), , vol., no., pp.1-7, 2-4 Aug. 2010doi: 10.1109/ISSA.2010.5588290http://ieeexplore.ieee.org.gate.lib.buffalo.edu/stamp/stamp.jsp?tp=&arnumber=5588290&isnumber=5588257

Ranganathan, C. and Brown C. V. (2006). “ERP investment and the market value of firms: Toward an understanding of influential ERP project variables,” Information Systems Research, No. 17(2), P. 145-161.

Roztocki, N. and Weistroffer, H.R. (2006). “Stock Price Reaction to the Investments in IT: Relevance of Cost Management Systems,” Electronic Journal of Information Systems Evaluation, 9, 1, 27-30.

Sellnow, T. L., Ulmer, R. R. and Snider, M. (1998). “The compatibility of corrective action in organizational crisis communication”, Communication Quarterly, 46: 1, 60 — 74

Song, Y. I., Woo, W. and Rao, H. R. (2007). “Interorganizational information sharing in the airline industry: An analysis of stock market responses to code-sharing agreements”, Information Systems Frontiers (2007) 9:309–324

Subashini, S., and Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications.

Symantec. (2011). State of Cloud Survey. Retrieved from: http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=stateofcloud2011

Tanna, G., Gupta, M., Rao, H. R. and Upadhyaya, S. (2005). “Information Assurance metric development framework for electronic bill presentment and payment systems using transaction and workflow analysis”. Decision Support Systems Journal, Elsevier publications, 2005. 41(1): p. 242-261.

Taylor, S., Christensen, T., Young, A., Kumar, N., and Macaulay, J. (2011). New Cisco IBSG Research Reveals Dramatic Growth in Cloud Interest Among SMBs. Retrieved from: http://www.cisco.com/web/about/ac79/docs/sp/SMB-Cloud-Watch-POV_IBSG.pdf

Telang, R. and Wattal, S. (2006). “Impact of software vulnerability announcements on the market value of software vendors - An empirical investigation.” Working Paper, Carnegie Mellon University, 2006

Trend Micro. (2011). Cloud Security Survey Global Executive Summary. Retrieved from:http://es.trendmicro.com/imperia/md/content/uk/about/global_cloud_survey_exec_summary_final.pdf

Tsiakis, T. and Stephanides, G. (2005). "The economic approach of information security," Computers & Security, Vol. 24, Number 2, 2005, pp. 105-108.

Yayla, A. and Hu, Q. (2005). “The impact of security breaches on the value of stocks: A shortterm vs. long-term perspective.”, In: The Annual Conference of IS in Asia-Pacific, (Las Vegas, NV., 2005).

Yildiz, M., Abawajy, J., Ercan, T., and Bernoth, A.: A Layered Security Approach for Cloud Computing Infrastructure, ISPAN, pp.763-767. In Proceedings of the 10th International Symposium on Pervasive Systems, Algorithms, and Networks (2009).

Yu, S., Wang, C., Ren, K., & Lou, W. (2010). Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing. 2010 Proceedings IEEE INFOCOM, (March), 1-9. Ieee. doi:10.1109/INFCOM.2010.5462174