Decision Support Systems 64 (2014) 67–78

Contents lists available at ScienceDirect

Decision Support Systems

journal homepage: www.elsevier.com/locate/dss

Do phishing alerts impact global corporations? A firm value analysis

Indranil Bose [a,*], Alvin Chung Man Leung [b,1]

[a] Indian Institute of Management Calcutta, Diamond Harbour Road, Joka, Kolkata 700104, India
[b] Department of Information Systems, City University of Hong Kong, Tat Chee Avenue, Kowloon, Hong Kong

ARTICLE INFO

Article history:
Received 1 May 2013
Received in revised form 15 April 2014
Accepted 22 April 2014
Available online 6 May 2014

Keywords:
Abnormal returns
Event study
Financial holding companies
Firm value
Phishing
Trading volume

ABSTRACT

Phishing is a form of online identity theft that is increasingly becoming a global menace. In this research, we analyze the impact of phishing alerts released in public databases on the market value of global firms. Using a sample of 1942 phishing alerts related to 259 firms in 32 countries, we show that the release of each phishing alert leads to a statistically significant loss of market capitalization that is at least US$ 411 million for a firm. We propose a theoretical framework for analyzing the impact of threats on firm value, and determine that the negative investor reaction is strongly significant for alerts released in 2006–2007 and for those targeted to financial holding companies, and weakly significant for firms listed in the US. We derive and validate these results using a combination of event study, subsampling analysis, and cross-sectional regression analysis. Our research makes a contribution by providing a new model for conducting multi-country event studies. We also contribute to the information systems literature by quantifying the loss in market value caused by phishing, and provide compelling evidence to information security administrators of firms that urge them to adopt adequate countermeasures to prevent phishing attacks.

1. Introduction

"Cyber-crime has become a $105 billion business that now surpasses the value of the illegal drug trade worldwide." — David DeWalt, CEO of McAfee [67]

With an increasing number of Internet crimes, online security has become a major concern for the general public. Among various online frauds, phishing, "a form of social engineering in which an attacker attempts to fraudulently retrieve legitimate users' confidential or sensitive credentials by mimicking electronic communications from a trustworthy or public organization", is one of the biggest threats to the online community [50]. This online crime has grown tremendously in recent years. According to the Anti-Phishing Working Group (APWG) the number of phishing incidents has increased from 47,324 in the first half of 2008 to 126,697 in the second half of December 2009. Since its first appearance around 1995, phishing has spread all over the world affecting millions of customers and numerous firms. Fig. 1 shows how phishing attacks take place and various associated financial losses. The actual financial loss due to phishing attacks may be ten times more than the estimated numbers for direct loss due to the indirect and the opportunity loss inflicted by phishing — an estimate of which is unavailable in literature [41]. Indirect losses take the form of increased customer support to phishing victims as well as efforts of customers to deal with credit-rating agencies to prevent themselves from being blacklisted due to the attacks. According to Meg Whitman, the former CEO of eBay, phishing has caused deterioration of trust of online customers and impaired e-commerce [10]. Her concern about opportunity loss is supported by the fact that the rate of opening of legitimate emails has dropped by 20% [9], and in a survey 89% of the respondents expressed concern about phishing attacks [79].

Motivated by the lack of research on the indirect and opportunity loss of phishing and particularly the lack of analysis of the impact of phishing on a worldwide basis, we embarked on analyzing the impact of phishing on the market value of firms. We collected data on phishing alerts targeted to global firms that were released by anti-phishing organizations. These alerts either included emails that were being sent to customers of public companies or notifications about fake websites that were being set up to lure customers. Using the event study method, we determined the impact of such alerts on the market value of global public firms by evaluating the change in their stock prices and trading volume after the release of the alerts. We also determined the various factors that influenced the impact.

Phishing has been a subject of intense research recently. The social and legal responsibilities of phishing were studied by researchers [7,88]. Technical research on phishing included development of anti-phishing tools such as AntiPhish, which is a browser extension that generates warning messages when users give away personal information to fake websites [58], and BogusBiter, which is a browser extension that feeds fake user information to phishing websites [89]. In business focused research on phishing, researchers analyzed anti-phishing preparedness of Hong Kong banks [8] and identified antecedents for the

* Corresponding author. Tel.: +91 33 2467 8300; fax: +91 33 2467 8062.
E-mail addresses: indranil_bose@yahoo.com (I. Bose), aleung@utexas.edu (A.C.M. Leung).
[1] Tel.: +852 3442 8521; fax: +852 3442 0370.

http://dx.doi.org/10.1016/j.dss.2014.04.006
0167-9236/

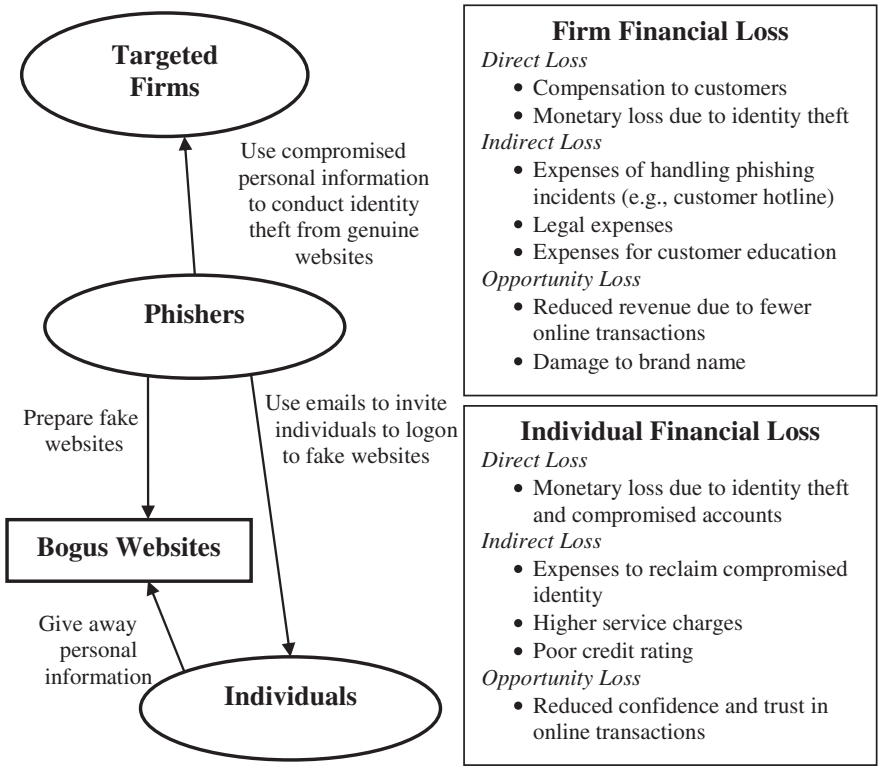

Fig. 1. Phishing attacks and their impacts on firms and individuals.

severity of phishing attacks [20]. Experimental studies discovered that user related behavioral and dispositional factors and phisher related social relationship mining skills led to success of phishing [49]. In summary, phishing has spurred enormous interest in academia and many anti-phishing tools and behavioral studies were conducted. Nevertheless, do industrial practitioners believe that the benefits of anti-phishing products justify the cost of adoption? This paper aims at providing a reasonable estimation of the loss in market value due to phishing. Through this study, we hope to arouse the awareness of managers to phishing and encourage them to adopt appropriate anti-phishing tools.

Our research is similar to past research conducted on information security breaches and their market impact. Using an event study, researchers showed that mishandling of confidential information [12], unauthorized access, hacking, denial of service (DoS), website vandalism [14], online credit cards thefts, website defacements [35], data breaches [36], and security breaches related to loss of integrity [52] caused a significant negative impact. The online nature of firms and tools used for attacks influenced the impact on firm value [2]. Prior research also reported negative but insignificant market reaction to DoS attacks [45]. Virus attacks resulted in contradictory positive and insignificant returns [46] as well as negative and insignificant returns [47] when different datasets were used.

The past research on the impact of security breaches examined only US firms. But there is no denying that security breaches in general and phishing attacks in particular are a global phenomenon. The insignificant market reaction observed in some prior studies could be due to the non-global nature of the research. Past research focused on discovering the link between security attacks and financial loss has often grouped various types of security breaches together [12,52]. Although DoS attacks and virus attacks have been studied separately [35,45,46], the impact of phishing on market value has not caught the attention of researchers. Phishing is a menace in its own right, and is different from other security breaches such as vandalism, DoS, and hacking. Those attacks are company oriented, and reveal the weakness of corporate security. On the contrary, phishing is customer oriented, and affects the perception of the customers about the targeted firm. This unique nature of phishing as a security breach motivates us to study its impact on global firms using 1942 alerts from 259 firms belonging to 32 countries. We also observe the lack of a theoretical framework in extant literature for studying the consequences of security breaches like phishing. We propose a risk-components based framework that explains why phishing causes a negative impact on firm value, and identifies factors at the firm, industry, country, and temporal levels that moderate the impact. Since our research involves firms from multiple countries, we improve on the traditional Capital Asset Pricing Model (CAPM) based event study method commonly used in Information Systems (IS) research, by proposing a refined asset pricing model that combines the Fama–French three factor model with the Fama–French international model, and is able to explain the risk in the cross-sectional abnormal return of global firms better. We conduct subsampling and cross-sectional regression to identify the significant moderating factors. Our results show that phishing alerts create statistically significant negative impact on stock prices and trading volume and lead to a loss of market capitalization that is at least US$ 411 million per alert. The market reaction becomes more pronounced for phishing alerts released in 2006–07 and for alerts targeted to financial holding companies. This research contributes to the literature on information security by quantifying the loss in market value caused by phishing, and providing hard evidence to security administrators to encourage adoption of adequate countermeasures to prevent phishing.

2. Theoretical framework

Our proposed framework for assessing the impact of security risks on market value of firms is shown in Fig. 2. According to Drucker, "risk is inherent to the commitment of present resources to future expectations" [27]. To model risk for a firm, we adapt the idea of risk-components proposed by Crockford [22]. The first component of risk is threats that can disrupt the functioning of an organization.

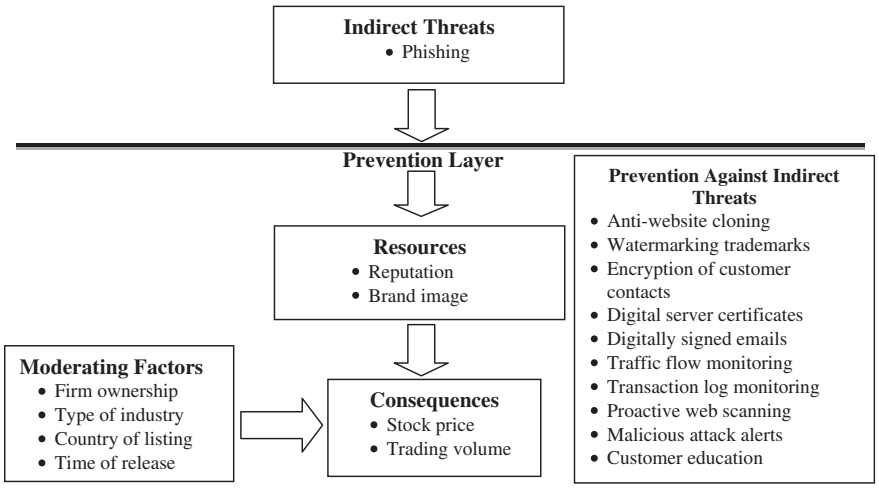

Fig. 2. Framework for analyzing the impact of indirect threats on firm value.

These can include direct or indirect "natural forces, human error, deliberate damage, and progressive deterioration" [22]. Phishing is an indirect security threat that manifests itself in the form of fake websites and spam emails and causes customers to give away their personal data.

Any threats acting on a firm can impact the tangible resources of the firm, such as physical properties, finances, and personnel, and intangible resources, such as reputation of firms, know-how of employees, and intellectual property rights of patents and designs [18,42]. In the case of phishing, the resources that are affected are the intangible resources of the firm such as reputation and brand name. Phishing is different from other forms of security breaches in that it is not targeted to a firm's computer system but to its potential customers. Despite the indirect nature, phishing can affect resources in the form of disrupted operations, loss of earnings, or deterioration of reputation. Although firms, whose customers are targeted through phishing, are considered to be victims in the eyes of law, most firms eventually compensate customers on a voluntary basis [50]. As a result, a phishing attack signals the message of potential future earnings loss for the targeted firm, that may be reflected in the stock price or trading volume.

The next important component of risk is the moderating factors that may be internal or external to the firms' resources, and can moderate the consequences of threats on the firm [86]. Since phishing is a global phenomenon and affects firms in multiple industries over time, four factors at the firm, industry, country, and temporal levels respectively are likely to determine the severity of impact of phishing. Phishers tend to attack as many customers of a firm as possible to improve their chances of success, and do not discriminate between customers of holding or subsidiary companies. However, the market reaction may be different for the different types of firm ownership, and this prompts us to list firm ownership as a moderating firm level factor. The type of industry can be quite relevant as phishing is mostly directed towards industries with the highest payoff [5]. Furthermore, the country of listing for firms influences the consequences of security threats due to a variety of reasons that include regulation, education, popularity of e-commerce, and awareness about security among the general public. Time plays an important role in influencing the impact of negative events such as security breaches [2,14,36] as concern about information security heightens as users become more knowledgeable about the crimes [63].

3. Hypothesis development

The consequences of phishing affect not only individual customers, but also corporate owners. To an extent, companies that are targeted by phishers are responsible for financial loss under specific ordinances. The US Truth in Lending Act requires companies to bear most of the losses due to unauthorized purchases [64]. The cost of lawsuits and potential compensation to customers may also drive down future profits of the companies. Furthermore, phishing incidents may undermine the confidence of consumers in using e-commerce services offered to them. Customers are sensitive to privacy issues and are concerned about trustworthiness of firms [28]. Prior research on information security has shown that customers' concern about security has driven down market value, and security breaches have given rise to a negative stock price return of 0.6% [1] and even an average loss in market capitalization of $1.65 billion per breach [14]. It is also known that confidentiality related security breaches [35], unauthorized access of confidential data [12], and software vulnerabilities associated with confidentiality breaches [84] have had a stronger impact on market value than other non-confidentiality related infringements. As phishing belongs to the class of confidentiality infringements, it poses a similar negative impact. This leads to:

H1. Phishing alerts cause a negative impact on return of stock price of targeted firms.

Phishing alerts may reduce the confidence of security conscious investors about the future prospect of targeted firms and influence them to sell their shares. The large amount of sell-off may cause significant changes in trading volume. Prior literature in finance has stated that while abnormal return of stock prices indicated the overall market expectations about an announcement, abnormal trading volume signified the change in the expectation of individual investors [15,54,57]. A joint test of both return of stock price and change in trading volume could enhance the power of the result generated from an event study [55]. e-Commerce investments [23], IT infrastructure investments [15], and IT investments from 1991 to 1996 [48] have generated significant positive increase in trading volume. At the same time, major negative events, such as the crash of the space shuttle Challenger, have triggered significant positive trading volume on the announcement day [66]. Phishing alerts will send a signal to investors to sell off shares of affected firms. This leads to:

H2. Phishing alerts cause positive abnormal change in trading volume.

In addition to studying the impact of phishing alerts on firm value, we also assess the moderating factors at the firm, industry, country, and temporal levels.

3.1. Firm ownership

Conglomerates with subsidiary firms are more likely to diversify their risks. Phishing as a risk may have less impact if it targets a subsidiary of a conglomerate. Prior studies have shown that the subsidiary status has a mitigating impact in case of data breach announcements [37] and DoS attack announcements [46]. The primary reason is that investors pay more attention to news that influences the overall profitability of a conglomerate and less attention to events related to a single subsidiary of a conglomerate. Though phishing may pose a negative impact on a targeted firm, its impact is less pronounced when targeted to a subsidiary of a conglomerate due to diversification of risk. This leads to:

H3. Phishing alerts targeting a subsidiary firm are likely to have less negative impact on the market value of the listed conglomerate which owns the firm than when it targets the conglomerate directly.

3.2. Type of industry

Dependency on IT varies from one industry to another. The financial services industry has higher requirements for IT infrastructure capabilities, IT management, and security services than production-based industries (e.g., manufacturing) [11]. Therefore, it is more sensitive to announcements related to IT, e-commerce, or outsourcing investments [23,26,48]. Phishers target industries with a heavy volume of monetary transactions, and over 90% of the reported phishing incidents are targeted to the financial services industry followed by the IT and telecom industry and the retail industry respectively [4]. Attacks targeted to credit unions experienced a tremendous year-to-year growth rate of 584%, followed by that of banks (325%) in the first two months of 2007 [37]. Firms that provide financial services are more concerned about legal, financial, and client risks in comparison to IT related and publishing related industries [80]. When faced with cyber attacks, the financial services industry may show a severe reaction because such attacks diminish the trust of customers and may even lead to legal proceedings from customers and regulators [76]. This leads to:

H4. Firms in the financial services industry are more negatively affected by phishing alerts than those belonging to other industries.

3.3. Country of listing

Due to its superb technological infrastructure, the US leads the world in the diffusion of e-commerce [38], and is also "the largest source of information security attacks" [77]. Online financial transaction is one of the key segments of B2C e-commerce in the US that has witnessed significant growth in recent years. Since more than 53 million people in the US conducted online banking around 2004–05 compared with about 15 million in the UK in 2007, people in the US tend to be more aware of phishing [29]. In a survey conducted by RSA, 83% of US bank account holders claimed to be familiar with phishing, whereas less than 70% of the interviewed bank customers in countries like Australia, the UK, and India made a similar claim [78]. Also, according to the APWG, most web-based phishing attacks are launched in the US and account for 37.25% of all attacks in January 2008, more than nearly three times the number of such attacks (11.66%) launched in the second highest ranking country [4]. Therefore, people in the US are more knowledgeable about the negative impact of phishing. Furthermore, the US has enacted specific laws against phishing. Federal laws include Identity Theft and Assumption Deterrence Act of 1998 and Social Security Number Privacy and Identity Theft Prevention Act of 2003 [50-51] and state laws include Anti-Phishing Act of 2005 in California and other similar laws in Texas and Arkansas [51]. By November 2008, the US Federal Government even mandated all banks to implement 'Red Flag Rules' to take a proactive role in detecting possible identity theft [7]. The strict anti-phishing laws may have heightened the awareness of the US investors about the negative impact of phishing.[2] Therefore, we posit:

H5. Companies listed in the US are more negatively affected by phishing alerts.

3.4. Time of release

Perception and awareness of the general public towards technology and its associated threats change over time [43,56]. In prior event studies, Im et al. found that recent IT investments resulted in more significant returns when compared with older investments [48]. Chatterjee et al. showed that recently announced new CIO positions resulted in a more statistically significant impact on firm value [16]. Benbunan-Fich and Fich demonstrated that the announcements related to traffic on websites created significant positive firm value in the pre-dotcom bubble period [6]. People's perception about security also changes over time. In the early 80s, people were more concerned about technical aspects of information security and in the late 90s, people focused on corporate best practices in information security management [85]. When analyzing the impact of security breaches on firm value, the reaction became more negative as time progressed [14]. Time also played a role in phishing. The number of individuals who received phishing emails increased from 57 million in 2004 to 124 million in 2007 [61]. With more frequent exposure to the news of phishing, the perception and knowledge of people also changed over time. This leads to:

H6. The negative impact of phishing alerts on firm value increases over time.

4. Research method and data analysis

According to McWilliams and Siegel, "an event is anything that results in new relevant information", and events in this research are phishing alerts released on public databases [68]. We collected data primarily from Millersmiles — the largest phishing alert database in the world with over 7000 announcements at the time of research. Since phishing alerts collected from a single database could be potentially biased and incomplete [70], we also collected alerts from alternative repositories such as Websense and from the websites of other region specific anti-phishing organizations, such as the Hong Kong Monetary Authority and Antiphishing Group Japan. Factiva, which is an international news database, was also used to cross-check and retrieve any remaining phishing alerts. Keywords such as phishing, fraudulent/bogus/fake email, fraudulent/bogus/fake websites, online identity theft, and scam were used. Appendix A shows some examples of phishing alerts retrieved from Millersmiles, Websense, and Factiva.

The data were collected from January 2003 to December 2007. We eliminated alerts related to private and non-listed public companies, duplicate alerts and alerts affected by confounding news about mergers/acquisitions, announcements of dividends/profits, change of management, new company development, and evaluation by external entities. We chose a confounding window of 5 days (2 days before, on, and 2 days after the date of phishing alert). The length of the confounding window was the longest among those used in prior event studies.[3]

Appendix B shows the breakdown of data collected from different sources before and after filtering. If a phishing alert recurred on a

[2] We compare the number of unique phishing alerts targeting US listed and non-US listed companies from 2003 to 2007. We find that as soon as the Anti-phishing Act was imposed in 2005, there was a sharp decrease in phishing alerts. More details can be found in online supplementary data Section E.

[3] Adopting a long confounding window may eliminate some sample data. However, it is a tradeoff to ensure that the changes in stock return and trading volume are due to phishing alerts rather than other confounding events because prior literature has shown that some announcements such as quarterly earnings announcements may have an impact on target firms for more than one day [60].

database or appeared on more than one database on different dates, only the earliest one was retained. We also ensured that each unique phishing alert for the same company was separated by at least three days.[4] A careful comparison of the description and snapshot of phishing emails, as well as address of websites available on phishing databases, was made to determine whether a phishing alert was unique. Furthermore, if the average stock price of a firm was less than US$ 1, or the average daily trading volume was less than 50,000 shares in the estimation period, then the corresponding alerts were eliminated [82]. We started with the retrieval of 9395 phishing alerts, and our cleaned dataset consisted of 1942 usable phishing alerts.[5]

4.1. Methods for event study

For determination of cumulative abnormal returns (CAR) of stock prices, the CAPM assumes linear relationship between the rate of return and the rate of market return, and is represented as:

$$R_{it} = \alpha_i + \beta_i R_{mt} + \varepsilon_{it}. \quad [6] \tag{1}$$

We used stock price data for 200 trading days that ended one month prior to the event announcement date, and built the regression models. In prior research, only one market index, such as S&P 500 index or CRSP Value Weighted Index was used. As our data involved firms from different countries, we considered multiple stock indices (including specialized indexes like the S&P banking index) for a particular stock, and chose the market index that resulted in the best adjusted R^2 for the regression model.

In past research, it was reported that the CAPM, which included only the market factor, resulted in miscalculation of abnormal market returns [32]. Fama and French determined that apart from the market factor, it was necessary to include two other factors that could explain the abnormal returns better [32,33]. They reasoned that there was a value premium in the average returns of stocks as analysts overvalued 'growth' (low book-to-market ratio and low earnings) stocks and undervalued 'value' (high book-to-market ratio and high earnings). Therefore, a risk factor (HML), that represented the difference between the high and low book-to-market ratio stocks in a value-weighted portfolio of stocks, should be added to the CAPM to compensate for the risk missed by that model. Similarly, when the book-to-market ratio was controlled, small firms generally had lower earnings than big firms. A second risk factor (SMB) was added to the CAPM, and represented the difference in the rate of returns between small and big firms in a value-weighted portfolio. Eq. (2) represents the Fama–French three factor model (FF):

$$R_{it} - R_{ft} = \alpha_i + \beta_i\left(R_{m_i t} - R_{ft}\right) + \gamma_i SMB_t + \delta_i HML_t + \varepsilon_{it}. \quad [7] \tag{2}$$

Besides finance, the FF model has been used to study the impact of branding [65], new product announcements [81], marketing alliances [83], and security breaches announcements [39] on market value.

However, it was not sufficient for us to use the FF model as is because the data consisted of several non-US firms. Past research on non-US markets had shown that when an international book-to-market correction factor (IHML) was added to the model, it could explain the returns generated from global value and global growth portfolios. The addition of one factor rather than two was done for simplicity, and Fama and French remarked that "we ignore other risk factors that might affect expected returns … our simple approach provides a reasonably adequate story for average returns" [34]. Such an international model was used to study the performance of hedge funds [13], but is yet to make its appearance in IS literature. We combined the three factor FF model for US data with the international FF model to develop the merged FF model (FFM) as shown in Eq. (3):

$$\begin{aligned} R_{it} - R_{ft} = \alpha_i + \beta_i = \left(R_{m_i t} - R_{ft}\right) + D_i(\gamma_i SMB_t + \delta_i HML_t) \quad [8] \\ + (1 - D_i)\phi_i IHML_{it} + \varepsilon_{it}. \end{aligned} \tag{3}$$

In this research, all stock prices and trading volume data were retrieved from Thomson Reuters. Daily data related to R_{ft}, SMB_t, HML_t, and $IHML_{it}$ were retrieved from Professor Kenneth French's website. Since the website listed $IHML_{it}$ for only 21 countries, 50 alerts from 11 countries not listed in that website were not analyzed.

We chose an event window of 3 days (one day before to one day after the release date of the phishing alert). The event window was kept short to conform with the assumption of efficient market, allow better power for the test statistics, and enable precise determination of confounding events [68]. Prior event studies have also chosen an event window of 3 days [2,12]. An impact on the day before the event was analyzed because there might be leakage about the phishing incident in online electronic media before it appeared in the database. For computation of the cumulative abnormal trading volume (CAV), the market adjusted model was chosen.[9] Our approach of choosing a mixed model for stock price and trading volume was similar to a prior study [15]. To test the statistical significance of the abnormal returns of stock prices and trading volume, a parametric Z test was used [26]. To further establish the robustness of results, we used non-parametric tests that are better in controlling "nonnormal distributions cross-sectional dependence and increases in the variance of abnormal returns during the event window" [15]. We used the sign Z test [19] and the Corrado's rank test [21].

4.2. Subsampling and cross-sectional regression

Similar to the composition of the reported phishing incidents of APWG, our sample data were primarily from US listed companies (64.4% of the total sample) and from the financial services sector (79.1% of the total sample). In order to minimize the potential sampling bias, we split the data into subsamples based on various moderating factors such as firm ownership (holding and subsidiary), country of listing (US and non-US), type of industry (financial services firms and others), and time of release (pre-2006 and 2006–07). These subsamples

[4] There are 136 firms with multiple phishing alerts from 2003 to 2007. We summarize all those firms in online supplementary data Section A.

[5] Appendix B summarizes different sources of phishing alerts and Appendix C shows industry classification of our sample data. Our sample data involve 32 countries in 7 continents. They include Africa: South Africa (2); Asia: Hong Kong (33), India (7), Japan (18), Kuwait (2), Malaysia (15), the Philippines (2), Qatar (1), Singapore (9), South Korea (1), and United Arab Emirates (4); Australasia: Australia (69); Eurasia: Cyprus (1) and Turkey (1); Europe: Austria (1), Belgium (1), France (22), Germany (4), Greece (3), Ireland (8), Italy (8), the Netherlands (1), Romania (2), Spain (17), Sweden (2) and the United Kingdom (403); North America: Canada (48), Mexico (3) and the United States (1250); South America: Brazil (2), Colombia (1) and Venezuela (1). The number in brackets represents the total number of alerts for each country. More detailed summary statistics are available in online supplementary data Section B.

[6] In Eq. (1) R_{it} is the rate of stock return for firm i on day t, R_{mt} is the rate of return of market index m on day t, α_i is the y-intercept, β_i is the slope that measures the sensitivity of R_{mt}, and ε_{it} is the disturbance term.

[7] In Eq. (2), R_{ft} is the risk-free return of US treasury bills on day t, SMB_t is the size correction factor, and HML_t is the book-to-market ratio correction factor.

[8] In Eq. (3), D_i is a dummy variable that takes a value 1 when the firm i is listed in a US stock exchange, and 0 otherwise, and $IHML_t$ is the difference of returns between high and low book-to-market ratio stocks in a value-weighted portfolio constructed for day t, and for the country where firm i is listed. The monthly $IHML$ data was converted to daily data. Data conversion is common in event studies, and the three month Treasury bill data was converted to daily risk-free rate in the study of the Australian stock market [30].

[9] Some market indices, such as the MIBTEL General Index and the Colombia SE General Index, did not contain the market related trading volume data. If the market model was used it would require some phishing alerts to be eliminated due to the lack of trading volume data for some market indices. By using the market adjusted model, we could retain all phishing alerts.

corresponded to hypotheses H3 to H6. We computed the CAR for all subsamples, and used parametric and non-parametric tests on them to test the hypotheses. As a post-hoc analysis, we built regression models, where control variables and hypothesized variables acted as the independent variables, and the CAR for the most significant event window was the dependent variable. The three unrelated control variables included firm size, history of prior phishing alerts, and riskiness of phishing alerts. Firm size was studied in extant literature [1,2,14,36,52,84], and measured as natural logarithm of total assets reported in the last month of the year before the release of the phishing alert. The attack history of the firm was similar to frequency of incidents that was studied in past event studies [3,36,84]. It is represented as $\ln(n + 0.5)$, where n was the number of occurrences of phishing alerts in the past [72]. This variable was chosen to control the impact of repeated phishing alerts. The severity of the phishing alert, similar to severity of a security breach, software vulnerability, web outage, or virus attack [3,14,40,47,84], was the third control variable. It was represented by a dummy variable, where 1 indicated a sophisticated phishing alert with risk level above medium, and 0 otherwise.[10] The sample size for cross-sectional regression analysis was 1865 because the total assets for some companies with delisted tickers were not available. All hypothesized variables were dummy variables.[11] The descriptive statistics for these alerts and the correlations are shown in Table 1. The correlations were found to be less than ± 0.65. We used quantile regression instead of OLS because it was robust to departure from non-normality of error terms, presence of outliers, and minimized cross-sectional and cross-correlational heteroskedasticity[12] [59].

5. Research findings

The average adjusted R^2 for the CAPM for the entire sample was 0.465, and that for the FFM was 0.483. With the inclusion of additional risk factors, the explanatory power of the model increased. Panel A of Table 2 shows that the impact was the most significant one day after the alert was released. The event window [−1] did not show a significant result, implying no serious news leakage. Multiple day event windows, like [0,1] and [−1,1], showed significant results at the 5% level for all tests. The loss in market capitalization was at least US$ 411 million.[13] Therefore, H1 is strongly supported. With regard to the impact on trading volume, both parametric and non-parametric tests showed significant negative change. Panel B shows that, except event window [1] that was barely significant at the 10% level in the sign test, all other event windows showed significant negative change at the 1% level. The volume of shares traded in all event windows was lower than usual, implying a general lack of confidence among investors. However, the change in the CAV was significant negative rather than positive. Therefore, H2 is rejected.

5.1. Subsampling analysis (SA)

The impact of the moderating factors for event window [−1,1] is shown in Table 3. As shown in Panel A, all tests for FFM indicated subsidiaries were significantly affected but the Z test for the CAPM did not indicate the same. Therefore, H3 is rejected. Panel B shows the industry effect. The p-values for the financial services firms in both tests were less than or equal to 0.05 for the CAPM and the FFM but were mostly insignificant for the non-financial services firms.[14] Therefore, H4 is supported. Panel C shows the country effect. US firms showed significant negative CAR at the 10% level for the tests used on both models. The mean CARs of alerts associated with US firms were more negative than those associated with firms in other countries. Therefore, H5 is supported. The time period of announcement was classified as early or late depending on the year of the announcement. Several countries made it compulsory for firms to adopt two-factor authentication by 2005, and this led to our choice of 2005 as the cutoff year. Panel D shows that the impact of phishing increased over time. The announcements made in 2006 and 2007 resulted in significant negative CAR for firms in both parametric and non-parametric tests conducted on both models. In the pre-2006 period, the mean and median CARs were positive in some models in sharp contrast to the observation in the later period. This indicated a change in perception of investors about phishing alerts over time. Therefore, H6 is supported. We conduct further robustness checks by breaking down industry, country of listing, and year of announcements into more precise levels. The results obtained are consistent with the reported findings.[15]

5.2. Interaction analysis

Since the nature of ownership of firm turned out to be insignificant in SA, we decided to explore it more fully in association with another hypothesized variable. This is in agreement with Oh et al. who remarked that "a lack of attention to interaction terms might account for the inconsistent results found in conventional event studies that have considered only the main effects" [73]. The statistically significant interaction results are shown in Table 4.[16] As shown in Panel A, holding companies in the financial services sector were significantly negatively affected by phishing alerts with p-values less than 0.1 for both models. The interaction variable consisting of the Holding and Recent factors showed a significant and negative coefficient, with p-values less than or equal to 0.02 as shown in Panel B. This showed that while Holding by itself was not a significant factor, it became so in the presence of the financial services factor or the recent time factor. Finance and Recent were both significant factors in determining negative market impact. Hence, it was not surprising to observe that their interaction also gave rise to significant negative reaction as shown in Panel C. Similarly, Panel D shows that the interaction of US and Recent also resulted in significant negative impact. Interestingly, although US and Finance were independently significant factors, their interaction turned out to be insignificant.

5.3. Cross-sectional regression analysis (CSRA)

To validate the findings in the SA, we conducted CSRA using data from the event window [−1,1] that showed the most significant negative CAR at the 5% level. In the QR results shown in Table 5, the control variables were insignificant for all models. Similar to a prior study [15], an OLS regression model constructed using all variables except the interaction terms showed that the variance inflation factor (VIF) was less than 3 for all variables. As VIF was less than 10, this indicated that

[10] For alerts listed from Millersmiles, the risk level was pre-determined, and for others, it was determined on the basis of their similarity to phishing alerts listed on Millersmiles.

[11] Holding (1 for holding firms and 0 otherwise), Finance (1 for financial services firms and 0 otherwise), US (1 for US listed firms and 0 otherwise), and Recent (1 for occurrence in 2006 or 2007 and 0 otherwise).

[12] The OLS regression residuals of our sample data show that the error terms are not normally distributed. Therefore, we use quantile regression in this study.

[13] The loss in market capitalization due to an individual event was computed by multiplying the abnormal return by the average stock price and the average number of outstanding shares [68]. For [−1,1], the CAPM determined that the average loss in market capitalization for targeted firms ranged from US$ 493 million (using mean CAR) to US$ 935 million (using median CAR), whereas according to the FFM, the loss ranged from US $ 411 million (using mean CAR) to US$ 522 million (using median CAR) per alert.

[14] We further split non-financial services industries into IT & Telecom and others and still find that the impact of phishing alerts on the financial services industry is more negative and significant than that on others.

[15] Results of additional subsampling analyses can be found in online supplementary data Section C.

[16] Of the six possible two-way interaction terms that could be derived from the four hypothesized variables, four resulted in statistically significant results as shown in Table 5. Due to limitation of space, the statistically insignificant results for the interaction terms Finance * US and Holding * US are not shown.

Table 1
Descriptive statistics and correlations between hypothesized and control variables.

Sample size = 1942	Min	Max	Mean	Std. dev.	Firm size	Attack history	Risk level	Holding	US	Finance	Recent
Firm size[a]	19.23	33.02	25.60	1.94	1						
Attack history[b]	−0.69	7.34	3.32	2.01	0.09	1					
Risk level	0	1	0.09	0.29	0.01	0.04	1				
Holding	0	1	0.47	0.50	−0.12	0.03	−0.02	1			
US	0	1	0.63	0.48	−0.45	0.21	0.07	0.01	1		
Finance	0	1	0.78	0.41	0.63	−0.29	−0.01	−0.30	−0.33	1	
Recent	0	1	0.62	0.49	0.19	0.28	−0.07	0.00	−0.12	0.14	1

[a] Size of the firm is calculated as *ln*(total assets) and is represented in US$.
[b] Attack history is calculated as *ln*(number of prior phishing alerts + 0.5).

Table 2
Stock price and trading volume reaction.

Panel A: reaction of stock price

Event windows	[−1]		[0]		[1]		[−1,0]		[0,1]		[−1,1]	
Models	CAPM	FFM	CAPM	FFM	CAPM	FFM	CAPM	FFM	CAPM	FFM	CAPM	FFM
Sample size	1942	1892	1942	1892	1942	1892	1942	1892	1942	1892	1942	1892
Mean CAR	0.00%	−0.01%	−0.01%	−0.01%	−0.03%	−0.04%	−0.01%	−0.02%	−0.05%	−0.05%	−0.05%	−0.06%
Z test p-value	0.39	0.28	0.08	0.14	0.03	0.01	0.12	0.12	0.01	0.01	0.02	0.01
Median CAR	−0.04%	−0.03%	−0.03%	−0.04%	−0.04%	−0.04%	−0.08%	−0.06%	−0.07%	−0.06%	−0.09%	−0.10%
Sign test p-value	0.13	0.14	0.22	0.13	0.08	0.05	0.08	0.01	0.01	0.01	0.01	0.03
Corrado's rank test p-value	0.34	0.18	0.11	0.14	0.06	0.02	0.12	0.08	0.03	0.01	0.03	0.01

Panel B: reaction of trading volume

Event windows	[−1]	[0]	[1]	[−1,0]	[0,1]	[−1,1]
Sample size	1942	1942	1942	1942	1942	1942
Mean CAV	−6.25%	−8.21%	−5.31%	−14.46%	−13.52%	−19.77%
Z test p-value	0.00	0.00	0.00	0.00	0.00	0.00
Median CAV	−7.86%	−9.23%	−3.41%	−17.20%	−12.60%	−18.80%
Sign test p-value	0.00	0.00	0.10	0.00	0.00	0.00
Corrado's rank test p-value	0.00	0.00	0.03	0.00	0.00	0.00

little multicollinearity between the variables and the models was valid. The low R^2 reported in Table 5 did not imply poor accuracy because low R^2 (often less than 3%) was common in prior event studies and other financial studies using daily stock data [16,24,25].[17]

Models C1 and F1 (Table 5), that studied the impact of control and hypothesized variables on the CAR, showed that Recent was significant and negative.[18] Since four interaction terms of the hypothesized variables showed statistical significance in the SA, we exhaustively experimented with them in CSRA.[19] Models C2 and F2 studied the impact of inclusion of the interaction term Holding * Finance. Apart from Recent, Holding, Finance, and Holding * Finance were all significant in these models. However, only the coefficients for Recent and Holding * Finance were negative. In models C3 and F3, we added two interaction terms, Holding * Finance and Finance * Recent. Similar results were observed for both models and the coefficients for Recent and Holding * Finance were consistently negative and significant. Surprisingly, the coefficient for Finance * Recent was significant and positive. In models C4 and F4, we replaced Finance * Recent with Holding * Recent. Holding * Finance again had the most significant negative coefficient, but the coefficient of Recent was negative and marginally insignificant with p-value equal to 0.19 in the CAPM and 0.16 in the FFM. The coefficient for Holding * Recent was negative but insignificant. In models C5 and F5, when we replaced Holding * Recent with US * Recent, the coefficients of Holding * Finance were negative and significant for both models, and those for Recent were negative and significant only for the CAPM. The impact of US * Recent in C5 and F5 was insignificant in both models, but it was positive for C5 and negative for F5.

The CSRA confirmed that Recent played a significant role in driving down firm value and gave strong support for H6. With regard to firm ownership, we could conclude from the SA and the CSRA that it had no significant impact and thus, H3 was rejected. As for industry and country effects, though the SA showed that both significantly impacted abnormal returns, the CSRA showed that the impact was not strong, and it lost its significance in the presence of other hypothesized variables. Hence, H4 and H5 were partially supported. An important finding was that the interaction of Holding and Finance was strongly significant in driving the negative reaction of firms, and this was consistent for both the CAPM and the FFM.

6. Discussion

This research provided evidence that phishing alerts caused negative abnormal returns of stock prices and negative abnormal changes in trading volume. The mean CAR was low when compared to event studies related to catastrophes, where the CAR ranged from −2.48% to −11.86% on the event day [66]. The trading volume reaction of phishing alerts was different when compared to that of catastrophes. The low trading volume in the event windows showed that investors became indecisive about the future performance of the targeted companies, and preferred to hold rather than sell or buy stocks [87].

We found that firm ownership was an insignificant factor, whereas the industry and the country of listing were weak moderating factors. The time of occurrence of alerts, and specifically if the alerts were

[17] In the event study of e-commerce related announcements [82], the CSRA model generated a low R^2 of 0.002.
[18] As a robustness test, we replace the indicator variable Holding by diversification entropy using the measure proposed by Palepu [74]. Recent is still negative and significant in both CAPM and FFM. The results of additional cross-sectional regression analysis can be found in online supplementary data Section D.
[19] We eliminated any regression model that resulted in a high VIF from further consideration. Due to lack of space, only the most interesting models with VIF less than 8 for all variables are shown in Table 5.

Table 3
Impact of moderating factors.

Panel A: moderating effect of firm ownership					Panel B: moderating effect of type of industry				
Models	CAPM		FFM		Models	CAPM		FFM	
Firm ownership	H	S	H	S	Type of industry	F	N	F	N
Sample size	889	1053	853	1039	Sample size	1536	406	1486	406
Mean CAR	−0.04%	−0.05%	−0.04%	−0.07%	Mean CAR	−0.03%	−0.11%	−0.06%	−0.05%
Z test p-value	0.04	0.12	0.03	0.09	*Z* test p-value	0.05	0.09	0.02	0.15
Median CAR	−0.10%	−0.08%	−0.04%	−0.15%	Median CAR	−0.08%	−0.21%	−0.12%	0.00%
Sign test p-value	0.05	0.05	0.45	0.01	Sign test p-value	0.01	0.20	0.01	0.22
Corrado's rank test p-value	0.13	0.08	0.12	0.03	Corrado's rank test p-value	0.04	0.26	0.01	0.46
Panel C: moderating effect of country of listing					**Panel D: moderating effect of time of release**				
Country of listing	US	OC	US	OC	Time of release	O	R	O	R
Sample size	1250	692	1250	642	Sample size	751	1191	736	1156
Mean CAR	−0.07%	−0.01%	−0.08%	0.00%	Mean CAR	0.03%	−0.09%	−0.02%	−0.08%
Z test p-value	0.06	0.09	0.01	0.25	*Z* test p-value	0.36	0.01	0.22	0.01
Median CAR	−0.08%	−0.11%	−0.11%	−0.10%	Median CAR	−0.01%	−0.14%	0.01%	−0.15%
Sign test p-value	0.05	0.04	0.05	0.19	Sign test p-value	0.47	0.00	0.28	0.00
Corrado's rank test p-value	0.08	0.11	0.01	0.25	Corrado's rank test p-value	0.34	0.01	0.35	0.00

H: Holding, S: Subsidiary, F: Finance, N: Non-finance, US: US listed firms, OC: firms listed in other countries, O: Old period (i.e., before 2006), R: Recent period (2006–07).

released in 2006 and 2007, showed a significantly strong negative impact on market returns. Undoubtedly, the perception of investors towards phishing alerts evolved over time and with the availability of more knowledge about phishing alerts, investors realized the serious nature of such incidents. Any firms targeted after 2005 gave rise to the perception that they were not well equipped or were not doing enough to handle this type of event. This finding is similar to that of Kannan et al. who reported that the impact of security breaches was significantly more negative in the period following the dot-com bust [52] and that of Cavusoglu et al. who determined that "investors reacted more harshly to the recent attacks" [14]. The US as a country of listing, turned out to be a weak moderating factor as its coefficient was insignificant and sometimes even positive in the CSRA. A probable explanation for this observation is that due to frequent exposure to phishing incidents, investors in the US may have become inert to phishing alerts and do not take them as a surprise any more. Financial services as a moderating factor showed a weak negative influence. This was in line with existing literature, where researchers did not find the financial services sector to be significantly impacted by privacy or security breaches [1,52]. However, the interaction term of Holding and Finance showed a consistently strong and statistically significant negative reaction in the SA and the CSRA. This is an interesting result because it showed that the combined effect of the two factors was significant in determining the negative impact of phishing alerts on firm value.

It is known that sometimes the latent relationship between variables was not additive but multiplicative in nature [177], and this turned out to be true in this case. The significance of the interaction terms highlighted the importance of studying interaction variables. This is an important theoretical finding which may be useful in guiding IT firm value research in the future.

We used two different models for conducting the event study in this research. To the best of our knowledge, this is the first time the FFM model is used in IS. Though the FFM is a more conservative model than the CAPM, it was a preferred approach as it allowed us to study global firms and "compensate for risk missed by the CAPM" [31]. Although the loss in market capitalization due to phishing alerts computed by the CAPM was higher than that obtained using the FFM, we found strong consistency in the results generated using both models.

6.1. Managerial implications

Through this research, we demonstrated that phishing had a significant negative impact on market value of global firms. In more recent years, the impact became more significant because investors

Table 4
Impact of interaction factors.

Panel A: interaction effect of Holding * Finance					Panel B: interaction effect of Holding * Recent				
Models	CAPM		FFM		Models	CAPM		FFM	
Firm ownership	HF	NHF	HF	NHF	Type of industry	HR	NHR	HR	NHR
Sample size	582	1360	546	1346	Sample size	552	1390	525	1367
Mean CAR	−0.02%	−0.06%	−0.02%	−0.05%	Mean CAR	−0.14%	−0.01%	−15.66%	−0.31%
Z test p-value	0.05	0.08	0.07	0.14	*Z* test p-value	0.01	0.17	0.01	0.30
Median CAR	−0.09%	−0.08%	−0.06%	−0.05%	Median CAR	−0.19%	−0.05%	−14.92%	−3.00%
Sign test p-value	0.02	0.06	0.05	0.18	Sign test p-value	0.00	0.16	0.01	0.30
Corrado's rank test p-value	0.07	0.11	0.06	0.18	Corrado's rank test p-value	0.02	0.22	0.01	0.35
Panel C: interaction effect of Finance * Recent					**Panel D: interaction effect of US * Recent**				
Country of listing	US	OC	US	OC	Time of release	O	R	O	R
Sample size	993	949	958	934	Sample size	706	1236	706	1186
Mean CAR	−0.07%	−0.02%	−5.14%	−3.98%	Mean CAR	−0.14%	0.01%	−0.14%	0.01%
Z test p-value	0.04	0.13	0.06	0.20	*Z* test p-value	0.04	0.10	0.06	0.17
Median CAR	−0.11%	−0.08%	−8.00%	−3.75%	Median CAR	−0.11%	−0.08%	−0.10%	−0.05%
Sign test p-value	0.00	0.25	0.02	0.34	Sign test p-value	0.02	0.09	0.08	0.15
Corrado's rank test p-value	0.02	0.35	0.02	0.36	Corrado's rank test p-value	0.03	0.20	0.02	0.29

HF: holding firms in financial services industry, NHF: firms other than HF, HR: holding firms with phishing alerts released in 2006–07, NHR: firms other than HR, FR: financial services firms with phishing alerts released in 2006–07, NFR: firms other than FR, UR: US listed firms with phishing alerts released in 2006–07, NUR: firms other than UR.

Table 5
Cross-sectional quantile regression results.

	Panel A: CAPM					Panel B: FFM				
Models	C1	C2	C3	C4	C5	F1	F2	F3	F4	F5
Size	0.0002 (0.0003)	0.0003 (0.0003)	0.0003 (0.0003)	0.0003 (0.0003)	0.0003 (0.0003)	0.0001 (0.0003)	0.0002 (0.0003)	0.0002 (0.0003)	0.0003 (0.0003)	0.0002 (0.0003)
Attack history	0.0001 (0.0002)	0.0001 (0.0002)	0.0002 (0.0002)	0.0001 (0.0002)	0.0001 (0.0002)	0.0002 (0.0002)	0.0002 (0.0002)	0.0002 (0.0002)	0.0001 (0.0002)	0.0002 (0.0002)
Risk level	−0.0012 (0.0012)	−0.0009 (0.0011)	−0.0008 (0.0012)	−0.0009 (0.0011)	−0.0008 (0.0011)	−0.0008 (0.0012)	−0.0009 (0.0012)	−0.0010 (0.0012)	−0.0006 (0.0011)	−0.0008 (0.0012)
Holding	0.0004 (0.0007)	0.0041*** (0.0016)	0.0051*** (0.0017)	0.0049*** (0.0018)	0.0041*** (0.0016)	0.0005 (0.0007)	0.0037** (0.0017)	0.0037** (0.0018)	0.0044** (0.0017)	0.0038** (0.0017)
Finance	0.0013 (0.0013)	0.0041*** (0.0015)	0.0035* (0.0019)	0.0038** (0.0016)	0.0038** (0.0016)	0.0019 (0.0013)	0.0042** (0.0017)	0.0022 (0.0020)	0.0039** (0.0016)	0.0043*** (0.0017)
US	0.0009 (0.0008)	0.0009 (0.0008)	0.0008 (0.0009)	0.0009 (0.0008)	0.0004 (0.0012)	0.0008 (0.0008)	0.0008 (0.0008)	0.0006 (0.0009)	0.0008 (0.0008)	0.0010 (0.0013)
Recent	−0.0018**	−0.0018**	−0.0055***	−0.0013 (0.0010)	−0.0020* (0.0012)	–	−0.0022***	−0.0057***	−0.0013 (0.0009)	−0.0017 (0.0013)
	(0.0008)	(0.0007)	(0.0015)			0.0021*** (0.0008)	(0.0008)	(0.0015)		
Holding * Finance		−0.0042**	−0.0051***	−0.0036* (0.0019)	−0.0042**		−0.0037* (0.0019)	−0.0040** (0.0020)	−0.0033*	−0.0037**
		(0.0018)	(0.0020)		(0.0018)				(0.0018)	(0.0019)
Finance * Recent			0.0041** (0.0017)					0.0045*** (0.0017)		
Holding * Recent				−0.0019 (0.0014)					−0.0015 (0.0013)	
US * Recent					0.0008 (0.0014)					−0.0004 (0.0015)
Constant	−0.0082 (0.0063)	−0.0132**	−0.0120* (0.0069)	−0.0132**	−0.0127**	−0.0041 (0.0064)	−0.0099 (0.0069)	−0.0076 (0.0072)	−0.0111*	−0.0100 (0.0070)
		(0.0062)		(0.0065)	(0.0064)				(0.0065)	
Sample size	1863	1863	1863	1863	1863	1815	1815	1815	1815	1815
Pseudo R^2	0.0026	0.0041	0.0051	0.0047	0.0041	0.0032	0.0042	0.0059	0.0047	0.0042

* Significant at the 10% level.
** Significant at the 5% level.
*** Significant at the 1% level.

increasingly expected firms to be well-prepared to face off phishing. Financial services firms were commonly targeted by phishers, and such firms had negative market returns. However, such a factor alone was not significant enough in determining the market reaction. The interaction analysis showed that holding companies in the financial services sector received the most significant negative impact when phishing alerts were released. At the same time, while Litan reported that the number of phishing attacks in the US rose by nearly 40% in 2008 [62], the impact of phishing alerts on the US listed firms was surprisingly not so significant. Alerts that were released after 2005 created a strong negative impact on firm value. This meant that firms that had not taken any steps to prevent phishing needed to do so immediately. The loss of market capitalization of the order of several hundred million US dollars, as estimated in this research, should be a clarion call to firms to improve on their anti-phishing countermeasures. Firms could adopt technologies that prevented cloning of websites or caused poorer quality to the cloned websites. Existing technologies include content encryption and digital watermarking. Interested readers may also refer to [7] for more details about other technologies (e.g., traffic flow monitoring and proactive website scanning) to detect web cloning and fraudulent websites. Furthermore, firms could collaborate with anti-phishing organizations and Internet service providers in identifying and taking down of phishing websites.

6.2. Academic implications

Our research enriched existing academic literature in information security. We revisited the risk-components model proposed by Crockford and used it to study the impact of a security threat like phishing on firm value. We demonstrated the importance of considering moderating factors, and also the interactions between these factors to determine the impact on firm value. Past research had shown that security breaches that directly affect a firm's computer systems, such as virus, worms, and DoS attacks, caused a negative reaction. Phishing is a security breach that indirectly impacted the firms by targeting their customers and tarnishing their intangible resources like reputation and brand name. Yet its impact on firm value was strongly statistically significant as well. This implied that this indirect online criminal activity should not be ignored.

Another important contribution was the use of the FFM in conducting the event study. Phishing is a global phenomenon, and a study of phishing cannot be complete by considering only US companies. In fact, the negative impact of phishing is strongly statistically significant for all global firms, but is weakly significant for US firms only. This demonstrates the importance of considering non-US firms for studying a global phenomenon like phishing.

Finally, we showed that to appropriately analyze the impact of events on firm value, it was important to conduct the event study using stock prices and trading volume together with the SA and the CSRA on the same data. Most past event studies in IS have sought validation from some of these methods, but not all. Kaplan and Duchon have favored an approach where “using multiple methods increases the robustness of results because findings can be strengthened through triangulation” [53]. The consistency in the results obtained using multiple methods in our research improved the validity of the analysis and strengthened the findings.

6.3. Limitations of the study

We were not able to study the impact of phishing alerts for private firms and government organizations, although a number of phishing alerts were targeted to them. This was due to the limitation of the event study because it only allowed us to study publicly listed firms. Firms listed in countries, which did not make the phishing alerts publicly available, could not be studied as well. This research also suffered from the typical limitation of an event study — the

assumption about efficient markets. Some deviation from this assumption was possible, and that could affect the results. Finally, there is no denying that phishing alerts are an indirect measure of phishing attacks. Moore and Clayton have rightly lamented that the best approach to estimate "phishing activity would be to measure the number of emails delivered into inboxes and subsequently read by individuals" and yet "this email data are not available" [71]. We used the date of release of the alert as the event day. However, it is possible that there was a delay in the release of the alert. Although we used a large window of confounding events to overcome this, still there could be inaccuracies in the data that we couldn't control.

7. Conclusion and future research

Using a framework grounded on risk-components, we showed that phishing alerts led to statistically significant decrease in stock prices and trading volume of firms from 32 countries. The decrease in firm value was strongly significant for financial holding companies, and for alerts released after 2005, and weakly significant for all firms listed in the US. We found that the release of each phishing alert could cause a loss of at least US$ 411 million in market capitalization for a firm.

Future researchers can include alerts from more countries and propose alternative metrics for analyzing private firms. It will be interesting to categorize phishing attacks based on their nature, such as pharming, spear phishing, vishing, and smishing, and study their impact. Alternative event study models such as the multiple index model can be used to control for firm heterogeneity [44]. Park has used such a model by adding the currency exchange rate factor and a global stock index factor to the CAPM for studying international alliances [75]. Furthermore, it will be interesting to study whether voluntary disclosures made by firms about phishing attacks and announcements about adoption of anti-phishing measures lead to positive changes in their firm value. Finally, we encourage future researchers to continue to use data on global firms to overcome the "paucity of IT business value research in this area" [69], and provide better validation to firm value analysis.

Acknowledgements

The authors thank Professor John Bacon-Shone, Director of Social Science Research Centre, The University of Hong Kong, for statistics advice and Thomson Reuters for retrieval of some delisted stock data. The second author also thank the generous financial support of Swire Group to sponsor his trip to attend International Conference on Information Systems (ICIS) 2008 and valuable feedback received from the conference.

Appendix A. Examples of typical phishing alerts

Phishing alert from Millersmiles about Barclays

Barclays Message ID 79673 — Barclays Account Expire Notification
Date Reported: 23rd October 2005
Risk Level: MEDIUM
Apparent Sender: Barclays
Return Address: <accounts@barclays.co.uk>
Email Format: HTML
URL of Web Content: http://www.ctpacket.com/securesuite/olb/p/LoginMember.do/BarclaysIBank.htm
Location: CT, US
Detailed server information: www.ctpacket.com detailed server information
Comments:
* Email asks you to confirm/update/verify your account data at Barclays by visiting the given link. You will be taken to a spoof website where your details will be captured for the phishers.
* Barclays never send their users' emails requesting personal details in this way.
* The REAL URL of the spoof website is disguised as "https://ibank.barclays.co.uk/olb/p/LoginMember.do".
* The REAL URL of the spoof website looks nothing like the actual Barclays URL.
Content Email:
"We have noticed that you haven't used our online service recently, and we don't want you to miss out on the fantastic services available to you."

Phishing alert from Websense about Monster.com

Date: 03.28.2005
Threat Type: Phishing Alert
Websense® Security Labs™ has received reports of a new phishing attack that targets customers of Monster.com.
Users receive a spoofed email from the Monster Customer Support department saying that their account has been suspended, and they need to login to check their information.
This attack appears to be targeting companies who use the Monster.com Employers section. Employer users of Monster.com can post jobs on behalf of their company, and can search resumes in the Monsters database.
The phishing site is hosted in Korea and was up at the time of this alert.
Phishing email body:
Subject: Monster.com information
Dear Monster Customer,
We were unable to process the account is not suspended, please check your information by clicking here.
< URL REMOVED >
Monster Network < URL REMOVED > Customer Service
Phishing site screenshot

Phishing alert from Factiva about Wing Lung Bank

Title: Hong Kong: HKMA alerts members of fraudulent website
Date: 15 September 2006
Publication: The Asian Banker Interactive
The Hong Kong Monetary Authority (HKMA) wishes to alert members of the public in Hong Kong to a fraudulent website with the domain name "www.winglungservice.com". The website looks similar to the official website of Wing Lung Bank Ltd. (Wing Lung Bank). Wing Lung Bank has clarified that it has no connection with the fraudulent website.
Wing Lung Bank has reported the case to the Hong Kong Police Force for further investigation. Anyone who has provided his or her personal information to the website or has conducted any financial transactions through the website should contact Wing Lung Bank at 2770 2112 and any local Police Station or the Commercial Crime Bureau of the Hong Kong Police Force at 2860 5012.

Appendix B. Sources of phishing alerts

Source	Before filtering of confounding news	After filtering of confounding news
Millersmiles	7407	1655
Websense	582	160
APWG JP	32	15
HKMA	113	30
MyCERT	24	8
Factiva	1207	67
Others	30	7
Total	9395	1942

Appendix C. Industry classification of sample data

Industries	Global Industry Classification Standard (GICS)
Financial services	Banking related GICS Asset management & custody banks, diversified banks, investment banking & brokerage, and regional banks Finance related GICS Consumer finance, diversified capital markets, other diversified financial services, specialized finance, and thrifts and mortgage finance Insurance related GICS Life & health insurance, multi-line insurance, and property & casualty insurance
IT & Telecom	Application software, communications equipment, computer hardware, data processing & outsourced services, diversified commercial & professional services, electronic equipment manufacturers, integrated telecommunication services, internet software & services, systems software, and wireless telecommunication services
Others	Broadcasting & cable TV, building products, casinos & gaming, food retail, human resource & employment services, hypermarkets and supercenters, internet retail, IT consulting & other services, movies & entertainment, multi-utilities, publishing, railroads, real estate management & development, semiconductors, and trading companies & distributors

Appendix D. Supplementary data

Supplementary data to this article can be found online at http://dx.doi.org/10.1016/j.dss.2014.04.006.

References

[1] A. Acquisti, A. Friedman, R. Telang, Is there a cost to privacy breaches? An event study, Proceedings of Twenty-seventh International Conference on Information Systems, 2006, pp. 1563–1580.
[2] F.K. Andoh-Baidoo, K.-M. Osei-Bryson, Exploring the characteristics of Internet security breaches that impact the market value of breached firms, Expert Systems with Applications 32 (3) (2007) 703–725.
[3] J.H. Anthony, W. Choi, S. Grabski, Market reaction to e-commerce impairments evidenced by website outages, International Journal of Accounting Information Systems 7 (2) (2006) 60–78.
[4] APWG, Phishing Activity Trends Report: Report for the Month of January, 2008, Anti-Phishing Working Group, 2008. 1–9.
[5] APWG, Global Phishing Survey: Trends and Domain Name Use in 2H2009, Anti-Phishing Working Group, 2010. 1–33.
[6] R. Benbunan-Fich, E.M. Fich, Effects of web traffic announcements on firm value, International Journal of Electronic Commerce 8 (4) (2004) 161–181.
[7] I. Bose, A.C.M. Leung, Unveiling the mask of phishing: threats, preventive measures, and responsibilities, Communications of the Association for Information Systems 19 (24) (2007) 544–566.
[8] I. Bose, A.C.M. Leung, Assessing anti-phishing preparedness: a study of online banks in Hong Kong, Decision Support Systems 45 (4) (2008) 897–912.
[9] A. Brandt, Phishing anxiety may make you miss messages, PC World 23 (10) (2005) 34.
[10] A. Broache, Ebay CEO: Phishers Threaten User Trust, ZDNet News, March 8th, 2007, http://news.zdnet.com/2100-1009_22-6165628.html.
[11] M. Broadbent, P. Weill, B.S. Neo, Strategic context and patterns of IT infrastructure capability, The Journal of Strategic Information Systems 8 (2) (1999) 157–187.
[12] K. Campbell, L.A. Gordon, M.P. Loeb, L. Zhou, The economic cost of publicly announced information security breaches: empirical evidence from the stock market, Journal of Computer Security 11 (3) (2003) 431–448.
[13] D. Capocci, G. Hubner, Analysis of hedge fund performance, Journal of Empirical Finance 11 (1) (2004) 55–89.
[14] H. Cavusoglu, B. Mishra, S. Raghunathan, The effect of Internet security breach announcements on market value: capital market reactions for breached firms and Internet security developers, International Journal of Electronic Commerce 9 (1) (2004) 69–104.
[15] D. Chatterjee, C. Pacini, V. Sambamurthy, The shareholder-wealth and trading-volume effects of information-technology infrastructure investments, Journal of Management Information Systems 19 (2) (2002) 7–42.
[16] D. Chatterjee, V.J. Richardson, R.W. Zmud, Examining the shareholder wealth effects of announcements of newly created CIO positions, MIS Quarterly 25 (1) (2001) 43–70.
[17] S. Chatterjee, A.S. Hadi, Regression Analysis by Example, 4th ed. Wiley-Interscience, Hoboken, N.J., 2006
[18] S. Chatterjee, B. Wernerfelt, The link between resources and type of diversification: theory and evidence, Strategic Management Journal 12 (1) (1991) 33–48.
[19] H. Chen, M.Y. Hu, J.C.P. Shieh, The wealth effect of international joint ventures: the case of U.S. investment in China, Financial Management 20 (4) (1991) 31–41.
[20] X. Chen, I. Bose, A.C.M. Leung, C. Guo, Assessing the severity of phishing attacks: a hybrid data mining approach, Decision Support Systems 50 (4) (2011) 662–672.
[21] C.J. Corrado, A nonparametric test for abnormal security price performance in event studies, Journal of Financial Economics 23 (2) (1989) 385–396.
[22] N. Crockford, An Introduction to Risk Management, Woodhead-Faulkner, Cambridge, 1986.
[23] M. Dardan, A. Stylianou, S. Dardan, The valuation of ecommerce announcements during fluctuating financial markets, Journal of Electronic Commerce Research 6 (4) (2005) 312–326.
[24] B. Dehning, V.J. Richardson, A. Urbaczewski, J.D. Wells, Reexamining the value relevance of e-commerce initiatives, Journal of Management Information Systems 21 (1) (2004) 55–82.
[25] B. Dehning, V.J. Richardson, R.W. Zmud, The value relevance of announcements of transformational information technology investments, MIS Quarterly 27 (4) (2003) 637–656.
[26] B.L. Dos Santos, K. Peffers, D.C. Mauer, The impact of information technology investment announcements on the market value of the firm, Information Systems Research 4 (1) (1993) 1–24.
[27] P.F. Drucker, Management: Tasks, Responsibilities, Practices, 1st ed. Heinemann, London, 1974.
[28] J.B. Earp, A.I. Anton, L. Aiman-Smith, W.H. Stufflebeam, Examining Internet privacy policies within the context of user privacy values, IEEE Transactions on Engineering Management 52 (2) (2005) 227–237.
[29] B. Ensor, M.d. Lussanet, T.v. Tongeren, L. Camus, UK Online Banking Forecast: 2007 to 2012, Forrester Research, 2007. 1–17.
[30] R. Faff, A simple test of the Fama and French model using daily data: Australian evidence, Applied Financial Economics 14 (2) (2004) 83–92.
[31] E.F. Fama, Market efficiency, long-term returns, and behavioral finance, Journal of Financial Economics 49 (3) (1998) 283–306.
[32] E.F. Fama, K.R. French, The cross-section of expected stock returns, Journal of Finance 47 (2) (1992) 427–465.
[33] E.F. Fama, K.R. French, Common risk factors in the returns on stocks and bonds, Journal of Financial Economics 33 (1) (1993) 3–56.
[34] E.F. Fama, K.R. French, Value versus growth: the international evidence, Journal of Finance 53 (6) (1998) 1975–1999.
[35] A. Garg, J. Curtis, H. Halper, Quantifying the financial impact of IT security breaches, Information Management & Computer Security 11 (2) (2003) 74–83.
[36] K. Gatzlaff, K.A. McCullough, The effect of data breaches on shareholder wealth, Risk Management and Insurance Review, 2010. 61–83.
[37] S. Gaudin, Identity Theft Driven by Dramatic Spikes in Threats, InformationWeek, March 28th, 2007, http://www.informationweek.com/news/security/showArticle.jhtml?articleID=198700822.
[38] J.L. Gibbs, K.L. Kraemer, A cross-country investigation of the determinants of scope of e-commerce use: an institutional approach, Electronic Markets 14 (2) (2004) 124–137.
[39] S. Goel, H.A. Shawky, Estimating the market impact of security breach announcements on firm values, Information & Management 46 (7) (2009) 404–410.
[40] L.A. Gordon, M.P. Loeb, The economics of information security investment, ACM Transactions on Information and System Security 5 (4) (2002) 438–457.
[41] G. Goth, Phishing attacks rising, but dollar losses down, IEEE Security & Privacy Magazine 3 (1) (2005) 8.
[42] R. Hall, A framework linking intangible resources and capabilities to sustainable competitive advantage, Strategic Management Journal 14 (8) (1993) 607–618.
[43] A. Hawker, Security and Control in Information Systems: A Guide for Business and Accounting, Routledge, London, 2000.
[44] G.V. Henderson, Problems and solutions in conducting event studies, The Journal of Risk and Insurance 57 (2) (1990) 282–306.
[45] A. Hovav, J. D'Arcy, The impact of denial-of-service attack announcements on the market value of firms, Risk Management and Insurance Review 6 (2) (2003) 97–121.
[46] A. Hovav, J. D'Arcy, The impact of virus attack announcements on the market value of firms, Information Systems Security 13 (3) (2004) 32–40.
[47] A. Hovav, J. D'Arcy, Capital market reaction to defective IT products: the case of computer viruses, Computers & Security 24 (5) (2005) 409–424.
[48] K.S. Im, K.E. Dow, V. Grover, Research report: a reexamination of IT investment and the market value of the firm — an event study methodology, Information Systems Research 12 (1) (2001) 103–117.
[49] T. Jagatic, N. Johnson, M. Jakobsson, F. Menczer, Social phishing, Communications of the ACM 50 (10) (2006) 1–10.
[50] M. Jakobsson, S. Myers, Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft, Wiley-Interscience, Hoboken, N.J., 2007
[51] L. James, Phishing Exposed, Syngress, Rockland, Mass., 2005
[52] K. Kannan, J. Rees, S. Sridhar, Market reactions to information security breach announcements: an empirical analysis, International Journal of Electronic Commerce 12 (1) (2007) 69–91.
[53] B. Kaplan, D. Duchon, Combining qualitative and quantitative methods in information systems research: a case study, MIS Quarterly 12 (4) (1988) 571–586.
[54] J.M. Karpoff, A theory of trading volume, Journal of Finance 41 (5) (1986) 1069–1087.
[55] J.M. Karpoff, The relation between price changes and trading volume: a survey, Journal of Financial and Quantitative Analysis 22 (1) (1987) 109–126.
[56] V. Katos, C. Adams, Modelling corporate wireless security and privacy, The Journal of Strategic Information Systems 14 (3) (2005) 307–321.
[57] O. Kim, R.E. Verrecchia, Trading volume and price reactions to public announcements, Journal of Accounting Research 29 (2) (1991) 302–321.

[58] E. Kirda, C. Kruegel, Protecting users against phishing attacks, The Computer Journal 49 (5) (2006) 554–561.
[59] R. Koenker, K.F. Hallock, Quantile regression, Journal of Economic Perspectives 15 (4) (2001) 143–156.
[60] W.R. Landsman, E.L. Maydew, Has the information content of quarterly earnings announcements declined in the past three decades? Journal of Accounting Research 40 (3) (2002) 797–808.
[61] A. Litan, Phishing Attacks Escalate, Morph and Cause Considerable Damage, Gartner Research, 2007. 1–14.
[62] A. Litan, The war on phishing is far from over Gartner Research, 2009. 1–12.
[63] K.D. Loch, H.H. Carr, M.E. Warkentin, Threats to information systems: today's reality, yesterday's understanding, MIS Quarterly 16 (2) (1992) 173–186.
[64] J. Lynch, Identity theft in cyberspace: crime control methods and their effectiveness in combating phishing attacks, Berkeley Technology Law Journal 20 (1) (2005) 259–300.
[65] T.J. Madden, F. Fehle, S. Fournier, Brands matter: an empirical demonstration of the creation of shareholder value through branding, Journal of the Academy of Marketing Science 34 (2) (2006) 224–235.
[66] M.T. Maloney, J.H. Mulherin, The complexity of price discovery in an efficient market: the stock market reaction to the challenger crash, Journal of Corporate Finance 9 (4) (2003) 453–479.
[67] R. Martin, Cyberthreats Outpace Security Measures, Says McAfee CEO, InformationWeek, September 18th, 2007, http://www.informationweek.com/news/management/showArticle.jhtml?articleID=201807230.
[68] A. McWilliams, D. Siegel, Event studies in management research: theoretical and empirical issues, Academy of Management Journal 40 (3) (1997) 626–657.
[69] N. Melville, K. Kraemer, V. Gurbaxani, Review: information technology and organizational performance: an integrative model of IT business value, MIS Quarterly 28 (2) (2004) 283–322.
[70] T. Moore, R. Clayton, Examining the impact of website take-down on phishing, Proceedings of the Anti-phishing Working Groups 2nd Annual eCrime Researchers Summit eCrime 2007, 2007, pp. 1–13.
[71] T. Moore, R. Clayton, How Hard Can It Be to Measure Phishing? 2010. 1–4.
[72] E. Noma, D. Olivastro, Are there enduring patents? Journal of the American Society for Information Science 36 (5) (1985) 297–301.
[73] W. Oh, J.W. Kim, V.J. Richardson, The moderating effect of context on the market reaction to IT investments, Journal of Information Systems 20 (1) (2006) 19–44.
[74] K. Palepu, Diversification strategy, profit performance and the entropy measure, Strategic Management Journal 6 (3) (1985) 239–255.
[75] N.K. Park, A guide to using event study methods in multi-country settings, Strategic Management Journal 25 (7) (2004) 655–668.
[76] P. Petratos, Weather, information security, and markets, IEEE Security & Privacy 5 (6) (2007) 54–57.
[77] I.P.L. Png, C.Y. Wang, Q.H. Wang, The deterrent and displacement effects of information security enforcement: international evidence, Journal of Management Information Systems 25 (2) (2008) 125–144.
[78] P. Pradhan, Survey Shows Online Banking Needs Changes, Tech2.com India, January 29th, 2007, http://www.tech2.com/india/news/general/survey-shows-online-banking-needs-changes/3987/0.
[79] C. Saran, 90% of Online Adults Worried About Phishing, ComputerWeekly.com, August 30th, 2007, http://www.computerweekly.com/Articles/2007/08/30/226464/90-of-online-adults-worried-about-phishing.htm.
[80] D. Schoder, P.-L. Yin, Building firm trust online, Communications of the ACM 43 (12) (2000) 73–79.
[81] A. Sorescu, V. Shankar, T. Kushwaha, New product preannouncements and shareholder value: don't make promises you can't keep, Journal of Marketing Research 44 (3) (2007) 468–489.
[82] M. Subramani, E. Walden, The impact of e-commerce announcements on the market value of firms, Information Systems Research 12 (2) (2001) 135–154.
[83] V. Swaminathan, C. Moorman, Marketing alliances, firm networks, and firm value creation, Journal of Marketing 73 (5) (2009) 52–69.
[84] R. Telang, S. Wattal, An empirical analysis of the impact of software vulnerability announcements on firm stock price, IEEE Transactions on Software Engineering 33 (8) (2007) 544–557.
[85] B. von Solms, Information security — the third wave? Computers & Security 19 (7) (2000) 615–620.
[86] M. Wade, J. Hulland, The resource-based view and information systems research: review, extension, and suggestions for future research, MIS Quarterly 28 (1) (2004) 107–142.
[87] F.H. Westerhoff, Technical analysis based on price-volume signals and the power of trading breaks, International Journal of Theoretical & Applied Finance 9 (2) (2006) 227–244.
[88] R. Wetzel, Tackling phishing, Business Communications Review 35 (2) (2005) 46–51.
[89] C. Yue, H. Wang, BogusBiter: a transparent protection against phishing attacks, ACM Transactions on Internet Technology 10 (2) (2010) 1–31.

Indranil Bose is Professor and Group Co-ordinator of Management Information Systems at the Indian Institute of Management, Calcutta. He holds a B.Tech. from the Indian Institute of Technology, M.S. from the University of Iowa, and M.S. and Ph.D. from Purdue University. His research interests are in business analytics, information security, telecommunications, and business value of information technology. His publications have appeared in Communications of the ACM, Communications of AIS, Computers and Operations Research, Decision Support Systems, Ergonomics, European Journal of Operational Research, Information & Management, International Journal of Production Economics, Journal of Organizational Computing and Electronic Commerce, Journal of the American Society for Information Science and Technology, Operations Research Letters etc. He serves on the editorial board of Decision Support Systems, Information & Management, Communications of AIS, and several other IS journals.

Alvin Chung Man Leung is Assistant Professor at City University of Hong Kong. He received his Ph.D. from McCombs School of Business, The University of Texas at Austin. He obtained his BBA (Information Systems), BEng (Software Engineering), and Master of Philosophy degrees from the University of Hong Kong and MSc in Information, Risk, and Operations Management from the University of Texas at Austin. His research interests include social networks and information security. His works have been published in various journals and international conference proceedings such as Decision Support Systems, Communications of the Association of Information Systems, Communications of the ACM, and the International Conference on Information Systems.