Authors: Eva Szubartowicz and Guido Schryen
Manuscript accepted for publication in Journal of Information Systems Security

Timing in Information Security: An Event Study on the Impact of Information Security Investment Announcements

Abstract: Timing plays a crucial role in the context of information security investments. We regard timing in two dimensions, namely the time of announcement in relation to the time of investment and the time of announcement in relation to the time of a fundamental security incident. The financial value of information security investments is assessed by examining the relationship between the investment announcements and their stock market reaction focusing on the two time dimensions. Using an event study methodology, we found that both dimensions influence the stock market return of the investing organization. Our results indicate that (1) after fundamental security incidents in a given industry, the stock price will react more positively to a firm's announcement of actual information security investments than to announcements of the intention to invest; (2) the stock price will react more positively to a firm's announcements of the intention to invest after the fundamental security incident compared to before; and (3) the stock price will react more positively to a firm's announcements of actual information security investments after the fundamental security incident compared to before. Overall, the lowest abnormal return can be expected when the intention to invest is announced before a fundamental information security incident and the highest return when actual investing after a fundamental information security incident in the respective industry.

Keywords: *Event Study, Information Security, Investment Announcements, Stock Price Reaction, Value of Information Security Investments*

1. INTRODUCTION

As companies increasingly rely on technology to conduct their everyday business operations and deploy business strategies (Kankanhalli et al. 2003), the frequency and severity of corporate cyber-attacks and security breaches has increased and therefore information security has become a crucial concern for organizations. According to Forbes, the number of leaked records in the first half of 2017 is already higher than the number for all of 2016. Moreover, with over 4 billion, the number of records exposed in 2016 was already more than double the amount of both previous years combined (Forbes 2017). To protect a firm's valuable data and assets against these security incidents, organizations implement physical, technical or administrative security measures accordingly. By publicly announcing these information security investments, firms illustrate their ambition to provide their customers and partner firms with secure products and services. However, when it comes to information security investment announcements[1], timing plays a crucial role (Gordon & Loeb 2002; Tatsumi & Goto 2010; Xu et al. 2017): Firms need to decide whether to make the announcement before the investment, i.e., to announce the intention to invest in the near future or after the investment, i.e., to announce the actual investment. Studying the implications of firms' announcements of intended information security investments is beneficial for the following reason: With announcing the intention to invest and to implement information security countermeasures, firms may achieve a fast and immediate positive stock market return. However, the organization also discloses that it has not yet implemented that particular security countermeasure, therefore revealing a weakness and possibly open themselves to being attacked. Accordingly, an organization needs to carefully consider whether to pre-announce information security investments. Our study proposes that a firm's stock market value varies dependent on whether the announcement was before or after the actual investment, i.e., whether the firm announces their intention to invest or the actual investment.

Apart from the first dimension which focusses on examining the stock market reactions to announcements prior to investments and announcements after the investment, we analyse the stock market reactions to announcements prior to a fundamental security incident in a given industry and after. We strive to understand the effects of fundamental security incidents on the stock market's behaviour towards information security investment announcements. Research in this area is of particular importance for the following reason: Major security incidents such as the *Yahoo* hack in 2013, compromising 1.5 billion users' real names, email addresses and telephone numbers, attracted global attention and reinforced security fear among firms as well as individuals (Forbes 2013). After this major security incident an organization's announcement to invest in information security in order to increase the security level and to minimize the risk

[1] An announcement is defined as "*information supplied to the market, typically published in the press, by the managers of the firm*" [19].

of successful breaches and attacks enhances the confidence and trust of consumers and users in the investing firm. Therefore, we assume a different stock market reaction to a firm's announcement of security investments after and before a fundamental security incident. In this study, we regard different specific fundamental security incidents concerning various industries and compare the effect of information security investment announcements from firms of a given industry before and after an incident.

Overall, we regard timing in two dimensions, namely the time of announcement in relation to the time of investment and the time of announcement in relation to the time of a fundamental security incident. Thus, the first dimension deals with an endogenous phenomenon, since the organization is able to influence the time of announcement relative to the time of investment. The second dimension covers an exogenous phenomenon, since the firm cannot control the time of security incidents. For each time dimension we pose a research question (RQ):

RQ1: How do a firm's announcement of an information security investment intention and an announcement of an actual information security investment influence the firm's stock market value?

RQ2: How do a firm's announcement of an information security investment influence the firm's stock market value before a fundamental security incident and after the incident?

We examine the interplay between the endogenous and exogenous time dimension regarding information security investments, i.e., we study whether there is a correlation between the two research questions. For organizations, research in this area is of particular importance since it aids in the determination of the optimal point in time to invest in information security countermeasures.

The remainder of this article is organized as follows: In the next section we provide an overview of related work. Section 3 describes the hypotheses development. Subsequently follows the description of the research methodology we used in our event study. In Section 5 we present the results which are discussed thereafter. Moreover, managerial implications are described. The concluding section summarizes this work.

2. RELATED WORK

Academic work in the field of management information systems analysing the impact of security-related events on the market value of firms can be classified into two categories (Chai et al. 2011): (1) research focusing on the (negative) stock market impact resulting from information security breaches, incidents and vulnerabilities, and (2) research on the (positive) stock market impact caused by information security investments. Our study can be assigned to the second category.

Literature in the first category is numerous, focusing on IS breaches (Cavusoglu et al. 2004; Garg et al. 2003; Gatzlaff & McCullough 2010; Goel & Shawky 2009; Pirounias et al. 2014; Wang et al. 2013), loss of confidential data (Campbell et al. 2003), denial of service attacks (Hovav & D'Arcy 2003), virus attacks (Hovav & D'Arcy 2004; Wang et al. 2010), spam (Böhme & Holz 2006; Bouraoui 2009; Frieder & Zittrain 2007), and privacy violations (Acquisti et al. 2006). Moreover, the impact of information security breaches on the non-breached competitors has been studied (Aytes et al. 2006; Zafar et al. 2012). Generally, there are two main sources for information on the occurrence of security breaches: First, there are newspaper articles covering a firm's public announcement of a breach (Acquisti et al. 2006; Campbell et al. 2003; Cavusoglu et al. 2004; Goel & Shawky 2009; Hovav & D'arcy 2005; Hovav & D'Arcy 2004; Hovav & D'Arcy 2003); and second, there are various archives such as the Richardson's Stock Spam Effectiveness Monitor (Böhme & Holz 2006; Bouraoui 2009) from which reports can be downloaded. A detailed literature review on the impact of information security breaches on the stock market can be found in Böhme & Holz (2006) and Spanos & Angelis (2016).

The second category deals with the effects of information security investment events on the market. As a source of information, information security investment announcements from newspapers have been used (Bose & Leung 2013; Brock & Levy 2013; Chai et al. 2011; Jeong et al. 2016). In Table 1, literature on information security investment effects on the stock market is summarized.

Table 1 Research of Effects of Information Security Investments on Stock Market

Article	Research Focus	Key Findings
Chai [16]	Value of investments in IT security	- IT security investment announcements lead to positive abnormal returns for firms. - Security investments show higher abnormal returns after the Sarbanes–Oxley Act (SOX) than before.
Jeong [33]	Spillover value of investments in IT security	- IT security investment has negative effects on competitive firms' stock market values. - After the enactment of the Personal Information Protection Act, the competitors' stock market values respond more negatively to a security investment announcement than before the enactment.
Brock [13]	Value of e-banking investments in IT security	- E-banking firms making IT security investment announcements experience statistically significant market reactions.
Bose [11]	Value of implementing identity theft countermeasures	- Announcing the adoption of identity theft countermeasures increases the short-term market value of the announcing firm.

		- Early adopters, adopters of sophisticated identity theft countermeasures, firms with high growth potential, and firms with high credit rating experience a strong and positive return in market value, whereas small firms undergo a moderate positive reaction.
Xu [50]	Value of proactive and reactive IT security investments	- Proactive IT security investments for commercial exploitation increases stock market return - Reactive IT security investments for IT security improvement lead to higher returns than a commercial exploitation strategy
Deane [18]	Stock market's reaction to ISO 27001 certification	- Small organizations acquire greater benefits from the certification than large firms - More recent certification announcements result in more positive abnormal return than older certifications

While the negative financial impact of security-related events such as security breaches, attacks, and vulnerabilities was mainly advocated in academic literature (Acquisti et al. 2006; Campbell et al. 2003; Cavusoglu et al. 2004; Garg et al. 2003), an understanding of the positive financial impact resulting from information security investments is rarely analysed (Bose & Leung 2013; Brock & Levy 2013). According to various research studies, information security investments have a positive influence on the stock market value of the investing firm (Bose & Leung 2013; Brock & Levy 2013; Chai et al. 2011). The stock market's reaction to various types of information security investments has been regarded, e.g., investments in identity theft countermeasures or investments with commercial exploitation (Bose & Leung 2013; Chai et al. 2011; Xu et al. 2017). However, to the best of our knowledge, neither a distinction between intended and actual investments has been made, nor has the difference between announcements of intended and actual investments in terms of the impact on the stock market been analysed yet. This is true for both general IT investments as well as information security investments. Moreover, although existing academic research examined the stock market behaviour before and after the enactment of certain acts (Chai et al. 2011; Jeong et al. 2016), the stock market behaviour on information security investment announcements before and after fundamental security incidents has not been considered yet.

3. Hypotheses Development

In order to examine both RQ1 and RQ2, we analyse and compare the effects of four cases: (1) announcements of information security investment intentions before fundamental security incidents on the stock price, (2) announcements of actual information security investments before fundamental security incidents on the stock price, (3) announcements of information security investment intentions after fundamental security incidents on the stock price and (4)

announcements of actual information security investments after fundamental security incidents on the stock price. With comparing these four cases, we obtain four hypotheses which are developed in the following and depicted in Figure 1. In this study an organization's information security investment is categorized as *intended investment* if the organization announces its plans to implement a specific information security measure in the future, i.e., the measure has not been implemented up to the time of the announcement. On the other hand, if the firm publicly announces that it has successfully completed the implementation of an information security measure, i.e., if the security measure has been realized before the announcement, we categorize this announcement as an *actual investment*.

3.1. Comparison of Announcements of Actual Information Security Investments and Intentions

Publicly announcing the intention to commit to certain changes is common practice in some markets such as the airline industry and the chemical market (Achy & Joekes 2016; Besanko et al. 2009). Often, price changes or changes in the availability of products are pre-announced, i.e., they are announced before being put into practice (Achy & Joekes 2016). Reasons for price announcements in advance are to inform shareholders and customers, reduce the uncertainty that competitors will not follow, or to renege on price changes that competitors reject to follow (Besanko et al. 2009; Smith 2011). Accordingly, announcing the intention to implement specific actions and changes is strategically used by firms to observe customers' and competitors' reactions before actually implementing any alterations. In the context of information security investments, organizations frequently pre-announce the investments to gain strategic advantages or to attract customers with improved security systems. In this study we compare the effect of *intended* and *actual* information security investment announcements and hypothesize that compared to *actual* information security investment announcements, an *intended* information security investment announcement triggers a more negative stock market reaction; since an investment will be in the future, doubts whether the promised investment will be made persist. Moreover, with announcing information security investment intentions, a firm admits that imperfections regarding information security subsist and that there is potential for improvement. Accordingly, the announcing organization concedes that there are security vulnerabilities or weaknesses which will be fixed in the future but which are currently existent. In contrast, when a firm announces actual information security investments, the customers' and users' trust in the organization, its services and products increases because of knowing that the firm's security level is now higher than before and security incidents are less likely. We assume that this positive stock price reaction to an organization's investment announcement occurs independently of the time of announcement, i.e., before and after a fundamental security incident. We thus derive the following two hypotheses:

H1: *Before* fundamental security incidents, the stock price will react more positively to a firm's announcement of actual information security investments than to announcements of the intention to invest.

H2: *After* fundamental security incidents, the stock price will react more positively to a firm's announcement of actual information security investments than to announcements of the intention to invest.

3.2. Comparison of Announcements of Information Security Investments before and after fundamental security incident

Prior research studied information transfer in the context of information security, i.e., studies examined how a security incident in one firm affects the stock market prices of other firms (Ettredge & Richardson 2003). This effect can be negative (contagion effect) or positive (competition effect) (Laux et al. 1998). Research showed that organizations which were not actually attacked experienced negative stock return at the time when an organization in the same industry was attacked (Ettredge & Richardson 2003). We deduce that a security incident affecting one organization has an impact on the whole industry. Accordingly, we hypothesize that a fundamental security incident affects the corresponding industry in such a way that a security investment announcement after the incident causes a more positive stock return than before the incident. Consider the following scenario: After fundamental security incidents which have been publicly discussed and have caused a stir, investors' focus shifts to security considerations; realizing the extensive consequences of the security incident, investors may put more emphasis on security concerns in that industry than before the incident. Consequently, firms' information security investment announcements cause a more positive stock market return after a fundamental security incident in the corresponding industry than before, when security was considered less important and necessary. In order to prevent inconsistencies and overlaps with other fundamental security incidents, we separately regard various major security incidents concerning different industries. Accordingly, we consider different industry-specific fundamental security incidents. We hypothesize that after these incidents in the respective industry, information security and privacy concerns shift in the focus of investors' attention and therefore their reaction to information security investment announcements, whether intended or actual, is assumed to be considerably more positive than before the incident. Thus, we pose the following hypotheses:

H3: The stock price will react more positively to a firm's announcement of the *intention* to invest after a fundamental security incident compared to before.

H4: The stock price will react more positively to a firm's announcement of *actual* information security investments after a fundamental security incident compared to before.

Figure 1 presents the four hypotheses in a summarized form.

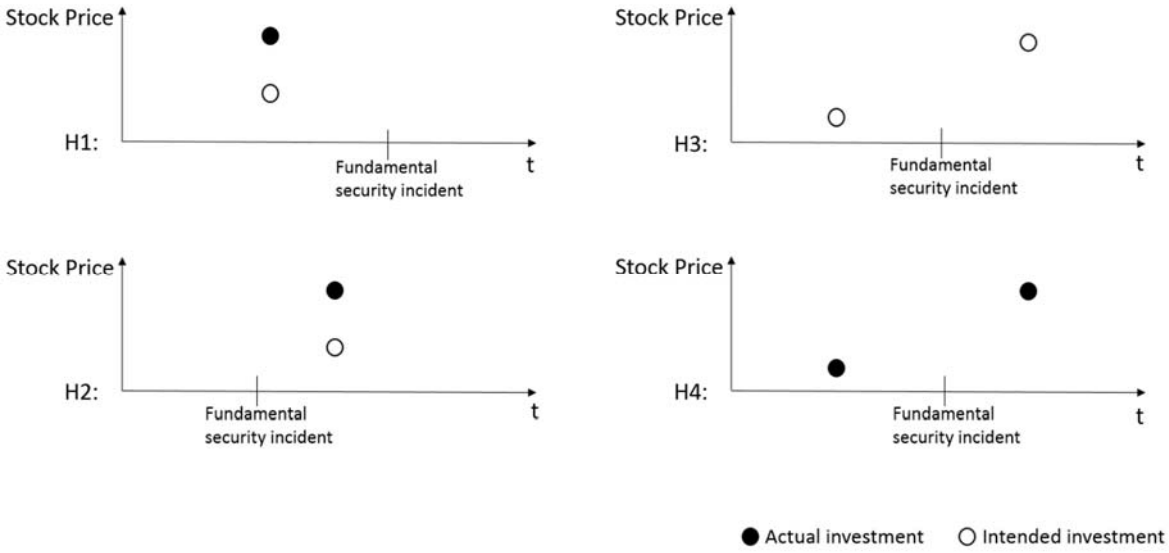

Figure 1 Presentation of the four Hypotheses

4. RESEARCH METHODOLOGY

This study uses an event methodology approach to investigate how market investors react to two types of information security investment announcements, i.e., actual and intended investments, before a fundamental security incident and after. The event study methodology is based on the efficient market theory, which states that when new information about an organization is publicly available, it is instantly absorbed by investors and incorporated into stock prices (Garg et al. 2003; Mortanges & Rad 1998). Thus, changes in stock prices reflect the impact of the new information provided on current and future firm performance (Garg et al. 2003). An event study, commonly used in accounting and finance literature (Dos Santos et al. 1993), is a suitable research method for studying the effects of public event announcements on stock prices since an immediate market response represents the expectations of investors towards a firm's future performance based on the current corporate actions (Bose & Leung 2013). Event studies are widely used in academic literature to examine the relationship between an IT-related event and its impact on an organization's value (Bose & Leung 2013; Campbell et al. 2003; Cavusoglu et al. 2004; Chai et al. 2011; Chatterjee & Carl Pacini 2002; Ranganathan et al. 2013).

4.1. Sample

We collected information security investment announcements by electronically searching the Lexis/Nexis Academic Database using the search terms “information security”, “security implementation”, and “today announce” covering the time period from 2000 to 2017. The elimination of announcements from private companies and non-listed public companies, whose stock returns cannot be assessed, as well as the exclusion of announcements which do not clearly state whether the investment has already been made or not, resulted in a sample consisting of 63 newspaper articles about information security announcements, i.e. we regard 63 investment announcements. Table 3 shows the distribution of our sample and Table 4 lists selected examples of information security announcements from our sample. The fundamental security incidents were extracted from breachlevelindex.com, an online database documenting data breach statistics based on publicly disclosed, worldwide security incidents. We acknowledge that security incidents occur on a daily basis. Therefore, we focus on fundamental breaches in various sectors of industry: We chose security incidents with the highest possible risk score of 10.0, i.e., breaches with an immense long-term impact and large amounts of highly sensitive information lost. Table 2 shows details on three exemplary incidents.

Table 2 Details on the Fundamental Security Incidents according to breachlevelindex.com

Breached Firm	Date of Breach	Industry	Risk Score
Equifax	07/15/17	Financial	10.0
Friend Finder Networks	10/16/16	Service	10.0
eBay	05/21/14	Retail	10.0

We determined a firm’s size according to the total number of employees at the time of the investment announcement (Size) (Arthur 2003; Ranganathan et al. 2013) c.f. Table 3. The industries of the announcing organizations were ascertained using their 4-digit SIC codes and were grouped into three industry types (*Industry*). To obtain historical data from the stock market we used Alpha Vantage, which offers APIs in a CSV format for real-time and historical stock data. Whether the investment is intended or actual (*Status*), and whether the type of security measure is human, technological or a certification (*Measure*) was extracted from the announcement articles. The date of announcement stipulates whether the announcement of a firm was made before or after the security incident has occurred in a given firm’s industry (*Incident*).

Table 3 Distribution of the Sample

Status	**Status of the announcement**	
	intended	22 announcements i.e., 34.9%
	actual	41 announcements i.e., 65.1%
Inciden	**Before/after security incident in particular industry**	
	before the incident	49 announcements i.e., 77.8%
	after the incident	14 announcements i.e., 22.2%
Measure	**Security measure the announcement refers to**	
	human	28 announcements i.e., 44.4%
	technological	12 announcements i.e., 19.0%
	certification	23 announcements i.e., 36.6%
Size	**Firm size of announcing firm**	
	small	21 announcements i.e., 33.3%
	medium	23 announcements i.e., 36.5%
	large	19 announcements i.e., 30.2%
Industry	**Industry of announcing firm**	
	Retail	6 announcements i.e., 9.5%
	Service	39 announcements i.e., 61.9%
	Financial	18 announcements i.e., 28.6%

Table 4 Examples of Announcements used in the Event Study Analysis

Company	Excerpt from Announcements	Type
Zoho	Zoho Corp. announced today that it has been awarded the ISO/IEC 27001:2013 certificate.	Actual
KDDI	Check Point Software Technologies Ltd., *[…]*, today announced KDDI, *[…]*, will incorporate Check Point VPN-1/FireWall-1(R) and Provider-1(R) into its new managed security service.	Intended
Humana	Network Associates, Inc., the leading provider of intrusion prevention solutions, today announced that Humana Inc. has selected McAfee(R) ePolicy Orchestrator(R) (ePO(TM)) 3.0.	actual
Royal Caribbean Cruises	Royal Caribbean Cruises Ltd. today announced the appointment of Renee Guttman as Chief Information Security Officer (CISO), effective January 25, 2016.	Intended
SEEK	Imperva, Inc., *[…]*, announced today that SEEK Limited has implemented Imperva SecureSphere Web Application Firewall (WAF).	actual

4.2. Statistical Methodology

In order to determine the impact of the investment announcements, we first estimate the stock return as if the announcement had not happened by means of an estimation window. To compute the expected return, we use the market model which is originally suggested by Markowitz (1968). The market model is a statistical model which links a firm's stock market return to the market index in order to form conditional predicted portfolio returns (Pettit & Westerfield 1974). It is the most common approach to estimate expected returns according to Bose & Leung (2013) and Dos Santos et al. (1993). It has been stated that simple models such as the market model are to be well specified and effective (Bouraoui 2009). The market model is based on the assumption that there is a linear relation between the stock market return of each firm and the return of the market index. Accordingly, the return R_{it} for firm i on day t can be expressed as a linear function:

$$R_{it} = \alpha_i + \beta_i R_{mt} + \epsilon_{it}. \quad (1)$$

In this study, the return R_{it} is computed from the stock prices obtained from Alpha Vantage (alphavantage.co) as the relative increase of the stock price over the price of the previous day; thus, we compute R_{it} by $R_{it} := \frac{Price_{it} - Price_{i(t-1)}}{Price_{i(t-1)}}$. Furthermore, R_{mt} is the return for the market on day t for which we used the Standard and Poor's (S&P) 500 index as done in prior event studies (Bose & Leung 2013; Hovav & D'arcy 2005; Hovav & D'Arcy 2003). The parameters α_i and β_i are the market model y-intercept and slope parameters for firm i, and ϵ_{it} is the disturbance term with ordinary least squares (OLS) properties[2].

For our study, we regard two windows, namely the estimation window and the event window as depicted in Figure 2. The estimation window is a time period with no event and is used to estimate the expected return. By contrast, the event window is a time period in which an event occurs and is used to calculate the abnormal returns. The two windows do not overlap. We set the event window for three days: the day prior to the announcement ($t = -1$), the day of the announcement ($t = 0$) and the day after ($t = 1$) as suggested by Dos Santos et al. (1993), Im et al. (2001), and Ranganathan et al. (2013). By including the day before the announcement, we capture market reactions caused by information leakage (Campbell et al. 2003). As an estimation window prior to the event we use the interval starting 122 days and ending 2 days before the event day as recommended in the literature (Campbell et al. 2003). Therefore, we use a discrete estimation window $T = [-122, -2], t \in T$ of 121 actual trading days.

[2] $E(\epsilon_{it}) = 0, Var\ (\epsilon_{it}) = \sigma_{\epsilon i}^2$.

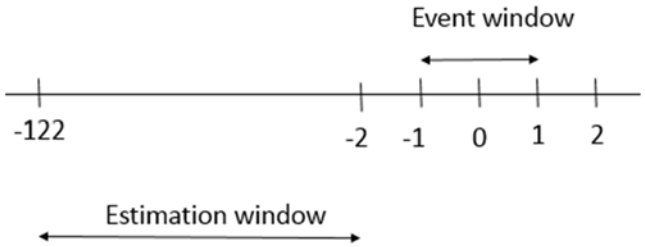

Figure 2 Timeline of Estimation and Event Window

The firm-dependent coefficients α_i and β_i from the market model (1) are estimated over the estimation window using linear regression, i.e., using data from before the event window; we estimate the expected returns and calculate what the normal returns would be at the day of the event for each event. With using data from before the event window we guarantee that the event does not distort the estimation of the expected returns. The estimated parameters "*remain fairly constant over long periods of time, e.g., the entire post-World War II period*" (Fama et al. 1969, p.403). This statement was backed up by the results on beta stationarity from Binder (1998), Blume (1971), and Lee & Wu (1985).
To determine the extent to which realized returns differ from expected returns due to investors' reactions to the announcement, we compute the abnormal rate of return AR_{it} for each day in the event window and for each event as follows

$$AR_{it} = R_{it} - \left(\tilde{\alpha}_i + \tilde{\beta}_i R_{mt}\right), \tag{2}$$

Thus, the abnormal return is the difference between the actual and the predicted return. Hereby, $\tilde{\alpha}_i$ and $\tilde{\beta}_i$ are the parameter estimates obtained by the regression of the market model (1) over the 121-day estimation window. To study the period surrounding the event date, we determine the cumulated abnormal return (CAR) over our three-day discrete event window $T = [-1,1], t \in T$ as the sum of the abnormal returns:

$$CAR_i = \sum_{t=-1}^{1} AR_{it}. \tag{3}$$

The average CAR for all events in the sample is computed with

$$CAR = \frac{1}{N} \sum_{i=1}^{N} CAR_i\,, \tag{4}$$

where N is the number of events in the sample.

We follow the approach of Chai et al. (2011) and examine influences caused by a firm's industry, size, or the implemented security measure on stock market return. To assess the impact of the variables on the CAR_i and to determine which variables play a significant role, i.e., cause changes in CAR, we used CAR as the dependent variable and ran a multiple linear regression model with

the control variables *industry*, *size* and *measure*. The independent variables are *incident* and *status*: As stated above, *status* refers to whether the announcement is intended or actual, and *incident* refers to whether the announcement was before or after the fundamental security incident in the particular industry.

$$CAR_i = \alpha + \beta_1 (Industry_{retail})_i + \beta_2 (Industry_{services})_i + \gamma_1 (Size_{medium})_i + \gamma_2 (Size_{small})_i + \delta_1 (Measure_{human})_i + \delta_2 \left(Measure_{technological}\right)_i + \zeta(Incident)_i + \eta(Status)_i + \epsilon_i. \quad (5)$$

Accordingly, *industry* refers to the industry sector (retail, service or financial), *size* refers to the firm size (small, medium or large), and *measure* refers to the security measure the firm announces to invest in (human, technological or certification). The parameters in the linear regression model were estimated using OLS. With the linear regression we show that the variables *industry*, *size* and *measure* do not influence the stock market return and therefore do not need to be considered when testing the hypotheses. In contrast, we show that the variables *status* and *incident* have significant effects on the stock market return.

To test hypotheses H1-H4, we split the data into subsamples corresponding to the criteria regarding timing (Bose & Leung 2013; Chatterjee & Carl Pacini 2002; Im et al. 2001), i.e., depending on the dimensions before and after the fundamental security incident in the particular industry and intended and actual information security investment announcements. This approach yields four subsamples, as shown in Table 6. For each hypothesis, we compare two of the subsamples against one another (cf. Table 6): We computed CAR for each subsample and applied two-sample t-tests, which are one of the most commonly used hypothesis tests and was already used in previous event studies (Agrawal & Kamakura 1995; Swanson 2011). In order to check for robustness, we repeated the analysis for a different discrete event window $T = [-2,2]$, as done in previous event studies (Bose & Leung 2013; Subramani & Walden 2001).

5. RESULTS

With regressing CAR we first examine the relationship between the CAR and event characteristics as described in the previous section. Thereafter, we test the statistical significance of differences in CAR for the subsamples corresponding to the four hypotheses H1-H4.

The results of the multiple linear regression (5) can be found in Table 5. The assumptions for OLS are satisfied[3]. The variables *status* and *incident* are significant in both event windows (0.065 and

[3] The assumptions “linearity in parameters” and “random sampling” are satisfied. Moreover, the expected value of the error term is zero, i.e., $E(\epsilon_i) = 0$ for all i because there is no relationship between the

0.042 in $t = [-1,1]$, and 0.077 and 0.022 in $t = [-2,2]$), i.e., changes in these variables are related to changes in CAR. Accordingly, we split the whole sample in subsamples corresponding to the variables *status* and *incident*. With p-values ranging from 0.361 to 0.821 in $t = [-1,1]$ and from 0.105 to 0.953 in $t = [-2,2]$, all control variables (firm *industry*, *size* and *measure*) were not significant in both event windows, which indicates that the abnormal returns corresponding to the announcements were not influenced by a firm's industry, size and the security measure that the firm invested in. Therefore, we do not consider the variables *industry*, *size* and *measure* in the following hypothesis tests.

Table 5 Regression Results

		$T = [-1,1]$			$T = [-2,2]$		
		Coefficient	t-score	p-value	Coefficient	t-score	p-value
Status (η)		-0.07343	-1.889	0.065	-0.03309	-1.814	0.077
Incident (ζ)		-0.02327	-1.365	0.042	-0.04325	-1.274	0.022
Control variable	Industry						
	-Retail (β_1)	-0.03804	-0.922	0.361	0.00211	0.059	0.953
	-Services (β_2)	0.01366	0.746	0.459	0.02596	1.656	0.105
	Size						
	-medium (γ_1)	-0.01531	-0.879	0.384	0.00314	0.211	0.834
	-small (γ_2)	0.00425	0.227	0.821	-0.01703	-1.061	0.295
	Measure						
	-human (δ_1)	0.00998	0.494	0.624	0.00481	0.278	0.782
	-technologic (δ_2)	-0.02354	-1.105	0.275	-0.00639	-0.416	0.679

parameters and the error terms ϵ_i. In order to proof that there is no multi-collinearity we showed that there is no linear relationship between the independent variables: We calculated the Pearson correlation coefficient in order to measure the correlation between two independent variables *status* and *incident*. For the computation we binary coded intended as 0 and actual information security investment announcements as 1. Announcements before the incident were coded as 1 and announcements after as 0. The correlation coefficient was found to be 0.069 and below the threshold level of 0.7. Therefore, there is no multi-collinearity. The last assumption we need to show is that there is homoscedasticity: To test whether the variance of the errors is constant we performed three tests, namely White test, Breusch-Godfrey test and Goldfeld-Quandt test. Heteroscedasticity was not detected.

The changes in stock prices for the subsamples and the results of the two-sample one-sided t-test by means of the T-score and its significance levels are shown in Table 6 and discussed in Section 6. The assumptions for the t-tests are satisfied[4]. The results indicate that the null hypothesis is rejected for H2-H4, i.e., we found evidence that hypotheses H2-H4 are supported.

Table 6 Impact of Information Security Investment Announcements Subsamples on Return of Stock Prices

		CAR (in %), SD		T-score	
		$T = [-1,1]$	$T = [-2,2]$	$T = [-1,1]$	$T = [-2,2]$
Panel A: Before fundamental security incident (n=49)					
H1	actual (n=33)	-1.8, 0.124	-0.1, 0.134	0.0919	0.8358
	intended (n=16)	-1.5, 0.040	-3.3, 0.060	(p=0.46)	(p=0.20)
Panel B: After fundamental security incident (n=14)					
H2	actual (n=8)	2.1, 0.120	2.6, 0.119	2.0952**	2.4227**
	intended (n=6)	0.7, 0.043	-0.1, 0.070	(p=0.03)	(p=0.02)
Panel C: Intended information security investment (n=22)					
H3	after incident (n=6)	0.7, 0.043	-0.1, 0.070	2.5596***	2.2722**
	before incident (n=16)	-1.5, 0.040	-3.3, 0.060	(p=0.01)	(p=0.02)
Panel D: Actual information security investment (n=41)					
H4	after incident (n=8)	2.1, 0.120	2.6, 0.119	2.9832***	1.8241**
	before incident (n=33)	-1.8, 0.124	-0.1, 0.134	(p=0.002)	(p=0.04)

The symbols *, ** and *** denote statistical significance at 0.10, 0.05 and 0.01 level respectively using a one-tail test. n is the number of announcements in the subsample. SD refers to the standard deviation.

[4] The assumption "independent samples" is satisfied. We used the Kolmogorov-Smirnov test to determine that the data is normally distributed. Moreover, the two samples have the same variance for each hypothesis: We ran the Levene's test for equality of variances and received p-values of 0.64, 0.07, 0.21 and 0.71 for the subsamples corresponding to hypotheses H1-H4 as given in Table 6. Therefore, the subsample variances can be treated as equal.

6. DISCUSSION OF RESULTS

In the following we discuss the results of the four hypotheses as presented in Table 6 in detail. Thereafter, the research questions RQ1 and RQ2 introduced in Section 1 are discussed and answered.

6.1. Discussion of the Hypotheses

6.1.1. Stock Price Reaction of Actual and Intended Information Security Investment Announcements Before Fundamental Security Incidents

Surprisingly, we did not detect a different stock market reaction for *actual* (-1.8% in $T = [-1,1]$ and -0.1% in $T = [-2,2]$) and *intended* (-1.5% in $T = [-1,1]$ and -3.3% in $T = [-2,2]$) information security investment announcements before fundamental security incidents (cf. Panel A of Table 6). The results of the t-test showed that the differences of intended and actual information security investment announcement are not significant and could have happened by chance. The null hypothesis is not rejected, as the type II error was $\beta = 0.46$ in $T = [-1,1]$ and $\beta = 0.20$ in $T = [-2,2]$. Overall, hypothesis H1 is not supported by our results.

Accordingly, before fundamental security incidents investors do not distinguish between intended and actual information security investment announcements. Before fundamental security incidents, they might not consider information security as worthy to invest in (Kankanhalli et al. 2003), and therefore they react similarly negative to both intended and actual information security investment announcements. Comparing the negative mean CARs with those of Chai et al. (2011) we notice that we obtain highly negative CARs in our study: The lowest CAR value regarding stock market reaction to information security investment announcements was -0.63% in Chai et al. (2011). We conclude that investors harshly punish intended information security investments before fundamental security incidents.

6.1.2. Stock Price Reaction of Actual and Intended Information Security Investment Announcements After Fundamental Security Incidents

In line with our expectations, the data analysis showed that investors react more positively to firms announcing actual information security investments than to organizations announcing intended investments after fundamental security incidents in the corresponding industry. After fundamental security incidents, actual information security investments clearly show high CARs in both event windows (2.1% in $T = [-1,1]$ and 2.6% in $T = [-2,2]$). Moreover, the results indicate that the CARs of actual information security investments are significantly higher than those of intended investments. This result is statistically significant in both event windows ($p < 0.05$ for both $T = [-1,1]$ and $T = [-2,2]$), as can be seen in Panel B of Table 6. The average

CARs for actual information security investments are higher than those for intended investments (0.7% in $T = [-1,1]$ and -0.1% in $T = [-2,2]$). Although the sample size was small, this study provides evidence that the stock market rewards companies' actual investments in information security after fundamental security incidents. The results, as shown in Panel B of Table 6, indicate that hypothesis H2 can be statistically confirmed.

This outcome reflects our assumption: Investors expect that actual information security investments result in increased revenue for the investing organization, as opposed to intended information security investments. Intended information security investments have yet to be implemented in the firm and can therefore not result in a higher security level. We assume that the fundamental information security incident in the particular industry causes the stock market investors to rethink the necessity of information security and raises awareness. Since hypothesis H1 could not be supported, i.e., before fundamental security incidents there is no significant difference between intended and actual information security investment announcements, fundamental security incidents cause a considerable change in the attitude of investors towards information security. In line with our assumption, the highest CAR can be expected when actually investing after a fundamental information security incident (2.6% in $T = [-2,2]$). Comparing the CARs of our study with those we notice that our CAR values are relatively low: Chai et al. (2011) obtain significant mean CAR values up to 4.49% resulting from information security investments which are announced after the enactment of SOX. Therefore, the observed changes in the stock market due to fundamental security incidents are comparatively small. A reason for these comparatively small values might be that we examine the stock market reactions of firms which are not directly affected by fundamental security incidents, but instead are in the same industry sector as the firm experiencing a breach. Moreover, we observe that the CAR value of actual information security investments remains rather stable over time (2.1% in in $T = [-1,1]$ and 2.6% in in $T = [-2,2]$), whereas the value for intended information security investments strongly decreases (0.7% in in $T = [-1,1]$ and -0.1% in in $T = [-2,2]$). We assume that, after fundamental security incidents, a firm's promise to invest in information security in the future is insufficient in the long term for investors whose security awareness has increased because of the incident: Investors appreciate the investment announcements at first but call for actual investments taking a long-term perspective. Return for actual investments remains stable because investors know that a firm's early investment in information security will increase the level of security within the organization in the long term.

6.1.3. Stock Price Reaction of Intended Information Security Investment Announcements Before and After Fundamental Security Incidents

As expected, regarding the percentage change in CAR, the gain for intended information security investments after fundamental security incidents in the respective industry is higher than the gain before an incident. Results shown in Panel C of Table 6 proof that, before the incident, highly

negative returns for intended investments take place (-1.5% in $T = [-1,1]$ and -3.3% in $T = [-2,2]$). Overall, hypothesis H3 is supported.

As discussed in Kankanhalli et al. (2003), investors might think that the risk of information security breaches is low and therefore see no use in investing in information security. Moreover, due to the difficulty of evaluating the benefits, they might be sceptical about information security effectiveness (Kankanhalli et al. 2003) and would have preferred investments in other business sectors, possibly resulting in increased revenues. We conclude that the fundamental security incident causes investors to acknowledge a firms' willingness to invest in information security even though the investment has not yet been made while being intended in the future. As predicted, firms' uncertain promises to improve their information security in the future are rewarded by investors after fundamental security incidents. The impact of information security incidents has been analysed from different perspectives: while the effect was negative for the breached firm (Acquisti et al. 2006; Campbell et al. 2003; Garg et al. 2003) and positive for its non-breached competitors (Jeong et al. 2016; Zafar et al. 2012), we found that firms from the same industry as the breached firm can benefit from the breach by announcing to implement information security countermeasures in the future. We observe that the mean CARs are distinctively smaller in $T = [-2,2]$ compared to $T = [-1,1]$. A reason for this might be investors awaiting another announcement claiming the promised information security measure has been implemented on day $t = 2$ and react negatively if there is no such announcement. After a fundamental information security incident, the stock market return even shifts from positive (0.7% in $T = [-1,1]$) to negative (-0.1% in $T = [-2,2]$) because information security has moved to the centre of investors' attention, and therefore investors punish those firms that do not keep their information security promises.

6.1.4. Stock Price Reaction of Actual Information Security Investment Announcements Before and After Fundamental Security Incidents

Panel D in Table 6 shows that, for actual information security investments, we observed positive abnormal returns after the fundamental security incident in both event windows (2.1% in $T = [-1,1]$ and 2.6% in $T = [-2,2]$). For actual information security investments, the results indicate that the CARs are significantly higher after a fundamental security incident in the particular industry than before in both event windows ($p < 0.01$ for $T = [-1,1]$ and $p < 0.05$ for $T = [-2,2]$). Before the incident, CARs are negative (-1.8% in $T = [-1,1]$ and -0.1% in $T = [-2,2]$). Overall, hypothesis H4 is supported.

This supports the assumption that fundamental security incidents in a certain industry shift investors' attitude towards information security in that industry: Before the incident investors do not approve spending money on information security because the necessity of information security is not recognized. After the incident the importance of information security in the corresponding industry is acknowledged. Since the investments are already implemented up to

the time of announcement, the investors are sure of the immediate increased security level of the announcing firm and reward it with higher CARs after an incident than before. The CAR in $T = [-2,2]$ is even higher than in $T = [-1,1]$ for investment announcements after incidents. We assume that the CAR increases two days after an incident because it may take two days to fully assess the severity of the damage caused by the fundamental security incident. When having fully realized the impact and seriousness of the incident, investors reward firms that aim at improving their security with even higher CARs than in $T = [-1,1]$. The conclusion that information security-related events impact the stock market returns regarding information security investments has already been drawn: After the enactment of SOX, the returns for information security investment announcements were significantly higher than before (Chai et al. 2011). We postulate that not only legislative efforts but also fundamental incidents increase information security awareness among investors and increase stock market returns of information security investment announcements.

In Table 7, we summarize the results of the discussion for each hypothesis.

Table 7 Summary of the Results for Hypotheses H1 - H4

Hypothesis		Result
H1	*Before* fundamental security incidents, the stock price will react more positively to a firm's announcement of actual information security investments than to announcements of the intention to invest.	not supported
H2	*After* fundamental security incidents, the stock price will react more positively to a firm's announcement of actual information security investments than to announcements of the intention to invest.	supported
H3	The stock price will react more positively to a firm's announcements of the *intention* to invest after the fundamental security incident compared to before.	supported
H4	The stock price will react more positively to a firm's announcements of *actual* information security investments after the fundamental security incident compared to before.	supported

6.2. Discussion of the Research Questions

6.2.1. Stock Price Reactions of Intended and Actual Information Security Investment Announcements

Our analysis shows that market reactions for intended and actual information security investment announcements are negative before fundamental security incidents, i.e., the stock market punishes both intended and actual information security investments before incidents in a given industry. Moreover, intended information security investments generate highly negative

stock market reactions before fundamental security incidents; however, there is no significant difference between actual and intended information security investments before fundamental incidents. The reason for this might be that information security investments are perceived to be big cost items without benefits. After a fundamental information security incident the situation changes. The status of investments, intended or actual, now plays a major role: In line with our expectations, the CARs of actual information security investments are significantly higher than those of intended investments after fundamental security incidents. We assume that the fundamental security incident causes investors to rethink the necessity of actual information security investments. The market rewards actual information security investments more generously and stock market investors expect greater benefits from actual information security investment than from intended investments. As intended information security investment announcements often generate negative abnormal stock returns (cf. Panel C in Table 6), we assume that investors disbelieve that the firm will keep its promises and implement the assured security countermeasures in the future. Another reason for the negative reaction to intended information security investment announcements could be that the announcing firm points out to the investors that the promised security countermeasure is not yet implemented within the organization, i.e., the current security level needs improvement. Therefore, the investors realize that the announcing firm is not sufficiently protected against security breaches. However, when regarding the temporal evolvement of the stock market reaction, i.e. regarding a slightly larger time frame, we observe instability of the stock market returns. Accordingly, no sustainable effects are caused: For all intended investments, whether before or after security incidents, the CAR value is always smaller in $T = [-2,2]$ than in $T = [-1,1]$. We assume that investors expect another announcement that the promised information security measure has been implemented on day $t = 2$ and react negatively if there is no such announcement. Accordingly, intended information security investment announcements lead to a short term rise in market returns, though quickly subsiding.

6.2.2. Stock Price Reactions of Information Security Investment Announcements Before and After Fundamental Security Incidents

For the question of how a firm's announcement of an information security investment influences the firm's stock market value before a fundamental security incident and after the incident, the results show that the fundamental incident influences the market reaction on information security investment announcements: Corresponding to our expectations, after the incidents, the CARs are distinctively higher than those before the incident (cf. Panel A and Panel B in Table 6), as the market rewards firms that try to improve their information security to prevent security incidents. Surprisingly, before the fundamental incidents the abnormal returns are negative and insignificant. After fundamental security incidents, the return for information security investment announcements, whether intended or actual, is positive and notably higher than for announcements before the incident, in which case negative CARs are returned. We assume that,

before fundamental incidents, investors do not recognize the necessity of information security investments, since they do not generate direct profit for the firm and they would prefer investments in more profitable business sectors instead: This may be why information security investments lead to negative CARs and therefore do not cause improvements of the organization's performance. This claim is backed up by academic literature: information security investments might not improve a firm's stock return (Chai et al. 2011; Dos Santos et al. 1993; Im et al. 2001). Those negative market reactions could be caused by investors' negative opinions or doubts about a firm's resource allocation or about its investment priority (Chai et al. 2011); i.e., investors may regard the investment in information security as superfluous. After fundamental security incidents in the respective industry, investors realize the importance of information security and believe that organizations investing in information security will improve their profit, reputation and popularity with customers. CAR values for actual information security investments after security incidents are lower in $T = [-1,1]$ than in $T = [-2,2]$ (cf. Panel B in Table 6).

However, as increased information security awareness is often limited in time (Allam et al. 2014; Kruger & Kearney 2006), we assume that this rise in investors' information security awareness is only temporary, has its peak instantly after the incident and decreases thereafter. Accordingly, there remains a need for research as to how investors' awareness evolves in the long term when more than one security incident in one industry sector is regarded. For future research, we recommend the development of approaches on how to raise stock market investors' security awareness so that they acknowledge firms' willingness to improve their information security not only after fundamental security incidents have occured.

6.3. Managerial Implications

For practitioners, this study provides useful insights and a true reflection on the return of information security investments: When an organization decides to invest in information security, it should take into consideration that actual information security investment announcements generate higher abnormal returns than intended ones. Thus, the organizations should wait to announce the investment until the information security measure has been implemented. Although intended information security investment announcements generate short-term increase of the stock market return, this return is rapidly decreasing. In contrast, actual information security investment announcements cause high abnormal return which are unstable over time. Accordingly, we recommend organizations to announce the actual investment in information security countermeasures and not the intention to invest.

Moreover, organizations should take into account that the stock market investors' interest in information security increases after a fundamental security incident in their industry. Accordingly, firms can expect a highly positive abnormal return if they announce their security investments after incidents and can therefore benefit from fundamental security incidents in

their industry. As a matter of course, firms might not be able to foresee fundamental information security incidents in their industry. Moreover, the line between "after incident *A*" and "before incident *B*" when regarding two incidents *A* and *B* in the same industry is blurry; put differently, organizations do not know whether they invest after the last incident or before the next one. For future work, we advise to study the stock market reaction of investing firms regarding two incidents in the same industry and to examine the line between "after incident *A*" and "before incident *B*".

Overall, the following guidelines can be derived: Firms should not announce their intention to invest before a fundamental security incident since this results in the lowest expected CAR. The highest CAR can be expected with actual investments after a fundamental information security incident in the respective industry.

7. CONCLUSION

This study provides evidence in support of the influence of information security investment announcements on an investing firm's market value. As described in the introduction, we regard timing in two dimensions, namely the time of announcement in relation to the time of investment and the time of announcement in relation to the time of a fundamental security incident. With reference to our research questions, we found that both dimensions influence the stock market return of an investing organization: Actual information security investments trigger a more positive stock market reaction after fundamental security incidents than intended investments. The return of actual information security investments is unstable and increasing one day after an incident, whereas the return of intended investments is decreasing. Moreover, we conclude that fundamental information security incidents in a particular industry increase the awareness of the importance of information security and arouse attention to information security investment announcements of firms in the respective industry. Our study shows that the stock market return of information security investment is often negative before fundamental security incidents. However, after an incident, we observe positive stock return for the investing organization.

The limitations of this study are related to the collected data: As we gathered the public information security investment announcements from newspapers, relevant information such as the amount of investment could not be included in our analysis. We assume that the amount of invested capital plays an important role on stock price returns: Investors might reward organizations that spend comparatively large sums with higher abnormal stock price returns than firms investing smaller sums or firms not investing at all. Furthermore, a larger sample size may improve the robustness of the results. Due to our screening process and our requirements on the data, we had to filter out a large portion of the announcements. With 63 information security investment announcements, we regard a relatively small size compared to, for instance, Brock & Levy (2013) and Chai et al. (2011). Nevertheless, since the results have been validated by a

statistical t-test conducted in two different event windows, the reliability of our findings is assured.

In this study, we differentiated between intended and actual information security investment announcements but did not consider the effects of the information security investments whose intention to invest has been pre-announced[5]. The reason for this is that firms do not announce *actual* investments if they have already (pre-)announced their *intention* to invest. Therefore, we were not able to assess the precise date of the pre-announced investment from the Lexis/Nexis Academic Database. Future research in the area of intended and actual information security investments should include the effects of pre-announced and subsequently undertaken investments, i.e., distinguish and compare the effects of intention announcements with the effects of the priory promised investment to the actual investment announcement. Moreover, academic research should study the implications of firms not keeping their promises to invest in information security even if they have already announced their intention to invest. Such research would benefit practitioners with answering the question which strategy to pursue when it comes to information security investment announcements, i.e., which order of actions is the most profitable.

[5] Assuming that the organization does keep its promise and implement the pre-announced information security investment.

REFERENCES

Achy, L. & Joekes, S., 2016. *Competition Policies and Consumer Welfare: Corporate Strategies and Consumer Prices in Developing Countries*, Edward Elgar Publishing.

Acquisti, A., Friedman, A. & Telang, R., 2006. Is There a Cost to Privacy Breaches? An Event Study. *ICIS 2006 Proceedings*, p.94.

Agrawal, J. & Kamakura, W.A., 1995. The economic worth of celebrity endorsers: An event study analysis. *The Journal of Marketing*, pp.56–62.

Allam, S., Flowerday, S.V. & Flowerday, E., 2014. Smartphone information security awareness: A victim of operational pressures. *Computers & Security*, 42, pp.56–65.

Arthur, M.M., 2003. Share price reactions to work-family initiatives: An institutional perspective. *Academy of Management Journal*, 46(4), pp.497–505.

Aytes, K., Byers, S. & Santhanakrishnan, M., 2006. The Economic Impact of Information Security Breaches: Firm Value and Intra-industry Effects. *AMCIS 2006 Proceedings*, p.399.

Besanko, D. et al., 2009. *Economics of Strategy*, John Wiley & Sons.

Binder, J., 1998. The Event Study Methodology Since 1969. *Review of quantitative Finance and Accounting*, 11(2), pp.111–137.

Blume, M.E., 1971. On the Assessment of Risk. *The Journal of Finance*, 26(1), pp.1–10.

Böhme, R. & Holz, T., 2006. The Effect of Stock Spam on Financial Markets.

Bose, I. & Leung, A.C.M., 2013. The Impact of Adoption of Identity Theft Countermeasures on Firm Value. *Decision Support Systems*, 55(3), pp.753–763.

Bouraoui, T., 2009. Stock Spams: An Empirical Study on Penny Stock Market. *International Review of Business Research Papers*, 5(4), pp.292–305.

Brock, L. & Levy, Y., 2013. The Market Value of Information System (IS) Security for e-Banking. *Online Journal of Applied Knowledge Management*, 1(1), p.1.

Campbell, K. et al., 2003. The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market. *Journal of Computer Security*, 11(3), pp.431–448.

Cavusoglu, H., Mishra, B. & Raghunathan, S., 2004. The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers. *International Journal of Electronic Commerce*, 9(1), pp.70–104.

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

Chatterjee, D. & Carl Pacini, V.S., 2002. The shareholder-wealth and Trading-volume Effects of Information-technology Infrastructure Investments. *Journal of Management Information Systems*, 19(2), pp.7–42.

Ettredge, M.L. & Richardson, V.J., 2003. Information Transfer among Internet Firms: The Case of Hacker Attacks. *Journal of Information Systems*, 17(2), pp.71–82.

Fama, E.F. et al., 1969. The Adjustment of Stock Prices to new Information. *International economic review*, 10(1), pp.1–21.

Forbes, 2017. How Can We Stop All These High-Profile Cyber Attacks And Security Breaches. Available at: https://www.forbes.com/sites/quora/2017/09/22/how-can-we-stop-all-these-high-profile-cyber-attacks-and-security-breaches/#17b735c37efe.

Forbes, 2013. Yahoo Account Hacked? How To Prevent Getting Hacked Again. Available at: https://www.forbes.com/sites/ericbasu/2013/06/26/help-my-yahoo-account-was-hacked-forensic-on-the-latest-yahoo-attack/#5509ef641dcd.

Frieder, L. & Zittrain, J., 2007. Spam Works: Evidence from Stock Touts and Corresponding Market Activity. *Hastings Comm. & Ent. LJ*, 30, p.479.

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

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

Goel, S. & Shawky, H.A., 2009. Estimating the Market Impact of Security Breach Announcements on Firm Values. *Information & Management*, 46(7), pp.404–410.

Gordon, L.A. & Loeb, M.P., 2002. The Economics of Information Security Investment. *ACM Transactions on Information and System Security (TISSEC)*, 5(4), pp.438–457.

Hovav, A. & D'arcy, J., 2005. Capital Market Reaction to Defective IT Products: The Case of Computer Viruses. *Computers & Security*, 24(5), pp.409–424.

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), pp.97–121.

Hovav, A. & D'Arcy, J., 2004. The Impact of Virus Attack Announcements on the Market Value of Firms. *Information Systems Security*, 13(3), pp.32–40.

Im, K.S., Dow, K.E. & Grover, V., 2001. A Reexamination of IT Investment and the Market Value of the Firm—An Event Study Methodology. *Information systems research*, 12(1), pp.103–117.

Jeong, S., Jeong, C.Y. & Lee, S.-Y.T., 2016. The Effect of Firms' Information Security Investment Announcements on Competitors' Market Values. , pp.300–307.

Kankanhalli, A. et al., 2003. An integrative study of information systems security effectiveness. *International journal of information management*, 23(2), pp.139–154.

Kruger, H.A. & Kearney, W.D., 2006. A prototype for assessing information security awareness. *computers & security*, 25(4), pp.289–296.

Laux, P., Starks, L.T. & Yoon, P.S., 1998. The Relative Importance of Competition and Contagion in Intra-industry Information Transfers: An Investigation of Dividend Announcements. *Financial Management*, pp.5–16.

Lee, C.F. & Wu, C., 1985. The Impacts of Kurtosis on Risk Stationarity: Some Empirical Evidence. *Financial Review*, 20(4), pp.263–269.

Markowitz, H.M., 1968. *Portfolio Selection: Efficient Diversification of Investments*, Yale university press.

Mortanges, C.P. de & Rad, A.T., 1998. Marketing Strategy and Market Value: An Event-study Analysis. *European Management Journal*, 16(3), pp.365–371.

Pettit, R.R. & Westerfield, R., 1974. Using the capital asset pricing model and the market model to predict security returns. *Journal of Financial and Quantitative Analysis*, 9(4), pp.579–605.

Pirounias, S., Mermigas, D. & Patsakis, C., 2014. The relation between information security events and firm market value, empirical evidence on recent disclosures: An extension of the GLZ study. *Journal of Information Security and Applications*, 19(4), pp.257–271.

Ranganathan, C., Ye, C. & Jha, S., 2013. Market Value Impacts of Information Technology Enabled Supply Chain Management Initiatives. *Information Resources Management Journal (IRMJ)*, 26(3), pp.1–16.

Dos Santos, B.L., Peffers, K. & Mauer, D.C., 1993. The Impact of Information Technology Investment Announcements on the Market Value of the Firm. *Information Systems Research*, 4(1), pp.1–23.

Smith, T., 2011. *Pricing Strategy: Setting Price Levels, Managing Price Discounts and Establishing Price Structures*, Nelson Education.

Spanos, G. & Angelis, L., 2016. The Impact of Information Security Events to the Stock Market: A Systematic Literature Review. *Computers & Security*, 58, pp.216–229.

Subramani, M. & Walden, E., 2001. The Impact of e-commerce Announcements on the Market Value of Firms. *Information Systems Research*, 12(2), pp.135–154.

Swanson, E.T., 2011. Let's twist again: a high-frequency event-study analysis of operation twist and its implications for QE2. *Brookings Papers on Economic Activity*, 2011(1), pp.151–188.

Tatsumi, K. & Goto, M., 2010. Optimal timing of information security investment: A real options approach. *Economics of Information Security and Privacy*, pp.211–228.

Wang, J., Xiao, N. & Rao, H.R., 2010. Drivers of Information Security Search Behavior: An Investigation of Network Attacks and Vulnerability Disclosures. *ACM Transactions on Management Information Systems (TMIS)*, 1(1), p.3.

Wang, T., Ulmer, J.R. & Kannan, K., 2013. The textual contents of media reports of information security breaches and profitable short-term investment opportunities. *Journal of Organizational Computing and Electronic Commerce*, 23(3), pp.200–223.

Xu, F. et al., 2017. Do Strategy and Timing in IT Security Investments Matter? An Empirical Investigation of the Alignment Effect. *Information Systems Frontiers*, pp.1–15.

Zafar, H., Ko, M. & Osei-Bryson, K.-M., 2012. Financial Impact of Information Security Breaches on Breached Firms and their Non-breached Competitors. *Information Resources Management Journal (IRMJ)*, 25(1), pp.21–37.