The financial impacts of information systems security breaches on publicly traded companies: reactions of different sectors

Received 15 November 2020
Revised 8 April 2021
Accepted 16 May 2021

Cansu Tayaksi
Center for Transportation and Logistics, Massachusetts Institute of Technology, Cambridge, Massachusetts, USA
Erhan Ada
Department of Business Administration, Yaşar Üniversitesi, Izmir, Turkey
Yigit Kazancoglu
Department of Logistics Management, Yasar University, Izmir, Turkey, and
Muhittin Sagnak
Department of Information Management, Izmir Katip Celebi University, Izmir, Turkey

Abstract

Purpose – Today, information systems and technology provides a wide set of tools for companies to increase the efficiency of their businesses. Although technology offers many benefits to businesses, it also brings risks as the information systems security breaches. Security breaches and their financial impact is a constant concern of the researchers and practitioners. This paper explores information systems breaches and their financial impacts on the publicly traded companies in different sectors.

Design/methodology/approach – After a comprehensive data collection process, data from 192 events are analyzed by employing Event Study Methodology and a comparison of the results between the four highly affected sectors (Consumer Goods, Technology, Financial and Communications) is presented. The abnormal returns on the prices of stocks after the events are calculated with the Market Model. Also, the results of the Market Adjusted Model and Mean Adjusted Model are presented to support the results.

Findings – While information systems security breaches have a significant negative impact on the Financials and the Technology sectors for all the event windows in the study ([−5, 0], [−5, 1], [−5, 5], and [−5, 10]), the significant negative impact is observed only on the [−5, 5] and [−5, 10] event windows for the Consumer Goods sector. No significant negative impact is observed in the Communications sector, in fact, the cumulative abnormal returns are positive for this sector.

Originality/value – The contribution of this paper to provide evidence about the financial impacts of the information systems breaches for businesses in different sectors. While there are studies that have previously focused on the information systems breaches and their financial impacts on businesses, to the best of our knowledge, this is the first study that compares this effect between the four highly impacted sectors. With a relatively larger sample size and broader event windows than the past studies in the literature, statistical evidence is provided to managers to justify their investments in information security and build preventive measures to secure the market value of their firms.

Keywords Information systems breaches, Cybersecurity, Event study methodology

Paper type Research paper

1. Introduction

Information technology (IT) is widely used in today's businesses to elevate the efficiency and the effectiveness of operations. While IT provides many advantages for companies, the increasing reliance on these technological advancements in business processes bring

Journal of Enterprise Information Management
© Emerald Publishing Limited
1741-0398
DOI 10.1108/JEIM-11-2020-0450

vulnerabilities to the critical infrastructures which result in risk exposure and information security breaches (Arcuri *et al.*, 2017; Amankwah-Amoah and Wang, 2019).

Information security breaches are major threats for businesses (Lab, 2012) and violations of the security of the information systems have costly effects for them (Sun *et al.*, 2006). Therefore, the organizations need to act more cautious to manage their information (Nishat Faisal *et al.*, 2007). For example, Facebook could face a fine of $1.63 billion due to the latest security breach that the firm experienced (Solon, 2018). In total, information systems security events cost almost $450 billion to the global economy every year (Arcuri *et al.*, 2017), the costs are doubled between 2013 and 2015 and quadrupled between 2013 and 2019 (Hamilton Place Strategies, 2015). With the COVID-19 Pandemic and increase in the number of employees that work from their homes, the opportunities increased for the attackers and the security event costs rose by 50% from 2019 to 2020 (Hiscox, 2020). Current digital technologies as artificial intelligence, the internet of things, cloud technologies and blockchain also brought vulnerabilities for the businesses for the cyber risk, which may total up to US$6 trillion in 2021 (World Economic Forum, 2020). The steep increase in the data breach cost displays that the cyber risk remains vital for businesses, and the importance of detecting information security vulnerabilities and taking preventive measures in organizations. The causes of the security breaches of information systems arise from weak data confidentiality and integrity and it leads to negative impacts on the operations and assets of the organizations (NIST, 2013). The security problems continue to happen despite the existence of numerous security guidelines and software for security evaluation and risk management. The threat and risk sources are hackers, malicious software, bad-tempered employees, rivals and other risk generators. Those threat agents originate internally or externally to an organization and all of them have diverse interests and motivations (Harris, 2010; Landoll, 2006).

Security breaches in an organization could harm the customer and business partners' trust and confidence. From the customer point of view, customers need perceived security by the business and any security concern is a barrier to the growth of a business (Alharbi *et al.*, 2013). For the business partners, after a business announces the security breaches to the investors, the firm value faces a risk to change based on the efficient market theory, i.e. the stock price of a business illustrates the existing information due to the "informationally efficient" nature of the markets (Fama, 1970). The anticipation would be a negative effect on net cash flows, thus the expected movement of valuations would be a decrease (Kannan *et al.*, 2007). Despite the anticipation of the negative impacts, companies are not spending enough resources to prevent information systems attacks (Richardson *et al.*, 2019). Companies still allocate less than 5% of their IT budgets to security-related challenges (Richardson, 2008) and only 50% of them are planning to increase their budgets (Ernst and Young, 2008). Hence, the research on this area is vital to help managers to realize the costs of cybersecurity breaches and understanding the exact impact of the security breaches on the stock market returns will help them to decide on their investment levels for the information security activities (Arcuri *et al.*, 2017; Gordon *et al.*, 2003; Goel and Shawky, 2009). The monetary amount that a business spends on the information security activities (from preventing to detect and correcting) should take a cost and benefits analysis as a basis (Gordon *et al.*, 2011). The cost and benefit information is vital to decide accurately on the investment levels, about the likelihood of the security incidents, and their future impact on the business value (Chai *et al.*, 2011). Managers would invest further in information security to prevent security breaches if they observed the investment is less than the loss in case of the event.

There is a research stream attempting to assess the financial impact of security breaches on businesses, based on the reactions of the market and change in the stock prices of the publicly traded firms (see Table 1). So far, the studies showed mixed results. Announcements of security breaches often, not always, result in a significant negative impact on the market returns of publicly traded companies (Richardson, 2019; Arcuri, 2017; Spanos and Angelis,

Author(s)	Year published	Data year(s)	Sample size	Results
Ettredge and Richardson	2003	2000	4	Significant negative impact
Acquisti *et al.*	2006	2000–2006	79	
Cavusoglu *et al.*	2004	1996–2001	66	
Aytes *et al.*	2006	1995–2005	67	
Goel and Shawky	2009	2004–2008	168	
Bolster *et al.*	2010	2000–2007	93	
Gordon *et al.*	2011	1995–2007	121	
Yayla and Hu	2011	1994–2006	123	
Gatzlaff and McCullough	2010	2004–2006	77	
Hovav and D'Arcy	2004	1988–2002	224	Insignificant positive impact
Hovav and D'Arcy	2003	1998–2002	23	Insignificant negative impact
Campbell *et al.*	2003	1995–2000	43	
Kannan *et al.*	2007	1997–2003	72	
Amir	2018	2010–2015	276	
Schuurman	2019	2016–2018	123	

Table 1. Summary of the financial impact of information system breaches

2016). While most of the studies found a significant negative impact on the stock prices after the announcement of the security breaches to a company (Campbell *et al.*, 2003; Aytes *et al.*, 2006; Gatzlaff and McCullough, 2010; Bolster *et al.*, 2010; Gordon *et al.*, 2011; Tanimura and Wehrly, 2015; Amir *et al.*, 2018, McShane and Nyugen, 2020), other studies found no negative impact or statistically insignificant negative impact on the companies. The reasoning behind the mixed results is mainly the short time-periods and relatively small sample sizes due to the nature of the topic (Yayla and Hu, 2011).

One of the questions in the literature is that "if security breaches create a negative financial impact, are all the businesses in the market facing it equally?" (Yayla and Hu, 2011). Tweneboah-Kodua *et al.* (2018) argue that the financial impacts of the information security breaches differ from business to business depending on its sector, therefore there is a need in the literature to examine the financial impacts of those events at a sectoral level. Smith *et al.* (2019) also suggest that studies should investigate if cybersecurity events are more effective in specific sectors. To the best of our knowledge, currently, there is limited research studying the financial impacts of these events for different sectors and existing literature mostly focuses on the financials sector. For example, Arcuri *et al.* (2017) studied the financial impacts of information security breaches by dividing their sample into two subsamples: "financial" and "other sectors," and Lagazio *et al.* (2014) focused on understanding the impacts of cybercrime on the financial sector. Malhotra and Malhotra (2011) studied the loss of market value after information breaches by dividing their sample into the finance and retail sector. While these studies indicate the importance of investigating the financial effects of such events at the sectoral level, in this paper it is argued that there is a need in the literature for the investigation of more sectors.

This study contributes to the growing literature on cybersecurity by providing evidence about the financial impacts of such events on the context of businesses in different sectors. In this study, a relatively large sample of events ($N = 192$) is analyzed for the years between 2000 and 2018 by using Event Study Methodology, and statistical evidence is provided to managers to justify their investments in information systems security and build preventive measures to security breaches to protect the market value of their businesses.

The remainder of this article's organization is as follows: Section 2 provides literature for earlier research on the information security breach events and their financial impacts on the companies. Section 3 presents the research methodology including the details of the data collection process and research model. Section 4 provides the results and discussions and Section 5 offers the managerial implications followed by the conclusions in Section 6.

2. Literature review

Information systems have a major role in the business world due to their capability of providing powerful managerial tools for the firms which help to achieve company goals. The Internet and information technology allows businesses to store, capture, process, share and manage a high amount of data (Bendovschi, 2015). However, despite the supporting nature of the information systems, they bring huge security threats to all businesses (D'Arcy *et al.*, 2014; SEC, 2018). Due to the constant development on the technological sides of the malevolent systems, information security is a continuously evolving research field both in academia and in the business world (Spanos and Angelis, 2016).

Information systems security is a vital topic that businesses are facing and there are always risks as accidental or unauthorized access, disclosure, or destruction of the system and the data. The managers are exposing their businesses to the risks without being aware, and they often refuse to acknowledge that the management process was poorly equipped (Loch *et al.*, 1992). The public awareness of the security breaches increased rapidly during the denial-of-service (DoS) attacks to the big Internet companies in 2000 where software developers became aware of the necessity of the security products (Markoff, 2002), and the investors' concerns are increasing about the publicly traded companies' exposure to the cyber risks (Spanos and Angelis, 2016). The rapid speed of the evolving new technologies such as artificial intelligence, data analytics, cloud systems, blockchain and many more, creates a more vulnerable environment for businesses (Amankwah-Amoah and Wang, 2019).

There is vast research on the technical and organizational features of the breaches of information systems; however, there is not enough attention to the economic impacts of the security breaches (Gordon and Loeb, 2002; Spanos and Angelis, 2016). Several studies analyzed the security breach announcements and their financial effects on the publicly traded firms by using Event Study Methodology. The first investigation discovered the relationship between the information security-related events and the impact on the stock price of the businesses was in the early 2000s. Despite the consensus about the negative impacts of information security-related events on the stock prices of publicly traded companies, there are still some conflicting views and mixed results in the literature (Amir, 2018). The majority of the studies agreed on the negative and statistically significant impact of the announcement of security on the stock prices of the company; however, despite the majority, some studies did not find any statistically significant negative impact on the market value (see Table 1).

Hovav and D'Arcy (2003) found insignificant negative results for all the firms after the occurrence of the DoS attacks and but significant negative results for the internet firms, indicating the Brick-and-Mortar businesses are not affected financially after the attacks. The authors later investigated the impacts with a much broader database; however, their study only focused on the virus attacks (Hovav and D'Arcy, 2004). The results were insignificant and mean abnormal returns were positive for the breached businesses. Kannan *et al.* (2007) and McShane and Nguyen (2020) also found insignificant negative overall impacts of security breaches. Campbell *et al.* (2003) pointed out that there is limited evidence of negative stock market reaction to the information security breach announcements, and further analysis exposed that the characteristics of the breach affect the result. Kamiya *et al.* (2020) demonstrated significant negative results for the businesses if only the attack resulted in a loss of personal financial information. Amir (2018) also found a quite small negative reaction to most cyberattacks in their sample as Kvochko and Pant (2015). Richardson *et al.* (2019) found limited economic consequences for the compromised companies, and the impact disappears shortly after the breach. They suggest the effect is on the economy-wide level rather than the individual company level. Also, Jeong *et al.* (2019) pointed that the security breach harms the business itself severely but creates a competitive environment for its competitor firms and results in a positive market return for them. Schuurman (2019) found no

significant impacts on the stock price after the announcement of the security breaches in the studied period for multiple event windows.

The most likely explanation of the conflicting views in the literature related to the impact of security-related events is the lack of big sample size (Acquisti *et al.*, 2006; Andoh-Baidoo and Osei-Bryson, 2007; Campbell *et al.*, 2003; Bose and Leung, 2013; Hogan, 2020). Researchers agree that a bigger dataset would yield an increase in the robustness of the findings, yet data collection about the security breach announcements is not trivial. The publicly traded firms are usually eager for making announcements about positive developments as e-commerce implementation initiatives, new mergers, and change in executive management but they are reluctant to share information when there is a security breach (Andoh-Baidoo and Osei-Bryson, 2007). Businesses have no incentive to announce to the public about the information security breaches and finding data is not so easy because not all the incidents are reported to the media and firms may tend to underreport the cyber-attacks (Campbell *et al.*, 2003; Amir, 2018). The announcement of the security breaches results mostly, not always, a negative impact on the market returns of the companies (Richardson, 2019; Arcuri, 2017; Spanos and Angelis, 2016).

Previous studies show that businesses in retail and technology sectors and more competitive sectors are reporting more vulnerable to information security breaches and reporting more events (Ettredge *et al.*, 2018; Amir *et al.*, 2018; Kamiya *et al.*, 2020) However, to the best of our knowledge, nearly none of the studies are focusing on the financial effects of information security breaches on a sectoral base (Acquisti *et al.*, 2006; Andoh-Baidoo and Osei-Bryson, 2007; Bolster *et al.*, 2010; Hovav and D'Arcy, 2003). As one of the few examples, Pirounias *et al.* (2014) divided their sample into two subsamples for analyzing the security breach impact as sector-based. Their sample consists of the technology and non-technology and financial and non-financial firms. However, they suggested that having a larger sample size and dividing the overall sample into sub-samples would yield more effective results. Since the majority of the research agrees on the significant negative impact of the information security breaches on the stock returns of the publicly traded companies, the following hypothesis is proposed in this study:

H1. Information security breach events create significant negative financial impacts on every sector.

In conclusion, the literature on the financial impact of security breaches on companies has increased since the early 2000s. However, it is still challenging for the researchers to agree on the impact level and achieve generalizable results. One of the missing elements of the information security breach-related studies is investigating the impact of these unexpected events on different sectors with relatively big sample size.

Thus, in this study, the financial impact of the security breaches on different sectors in the sample is analyzed. It is also argued, with this kind of information, the managers will have the opportunity to plan their security investments more effectively.

3. Methodology

Event Study is a quantitative approach for examining the effects of the company-related events on the market value of a business (Chaterjee *et al.*, 2001). The underlying principle of the methodology is based on the expectation of an unexpected event that will reveal a positive or negative response in the stock prices of a firm, thus the returns will become abnormal. The normal return estimation is calculated by the historical stock price returns and by subtracting the estimated normal return from the actual return, the abnormal return (AR) is obtained. If the results are positive, it is assumed that the impact of the events on the stock price of the firm is positive. Similarly, if the results are negative, it is assumed that the impact on the stock price is negative (MacKinlay, 1997).

The event study methodology is founded on the efficient market hypothesis (EMH) (McWilliams and Siegel, 1997). EMH of Fama (1970) offers a concrete foundation for the event study methodology by indicating the stock market is "informationally efficient" and the stock prices mirror the available information of a firm. If there is new information in the market, such as the new technology used in a firm, stakeholders will reflect their opinions on the firm's stock prices and there will be a change in the value of the firm (Fama, 1991). EMH suggests that the key mechanism behind price changes is the new information flow. If prices are adapting quickly and without prejudice to new information, the market is called "efficient". As a result, current prices of securities reflect any available information at any point in time. Based on EMH, it is expected that the publicly announced information security breach-related events will create a stock market reaction and that reaction would result in negative abnormal returns (Cardenas *et al.*, 2012). In this paper, the case of the new information arrival is the announcement of a security breach incident. In Figure 1, step-by-step description of the methodology is described.

3.1 Data collection

The first part of the methodology is the three-step data collection. In the first step, the security breach announcements are collected from a variety of resources. The resources for the data collection were prior studies; major newspapers of the US; magazines; and technology portals; a number of IT security-related blogs, various sources through the search engines Google and Yahoo! and the website of a nonprofit organization named Privacy Rights Clearinghouse. The search keywords were: "cyber-attack," "cybersecurity incidents," "information security breach," "information system incidents," "information system hack," "hacked companies,"

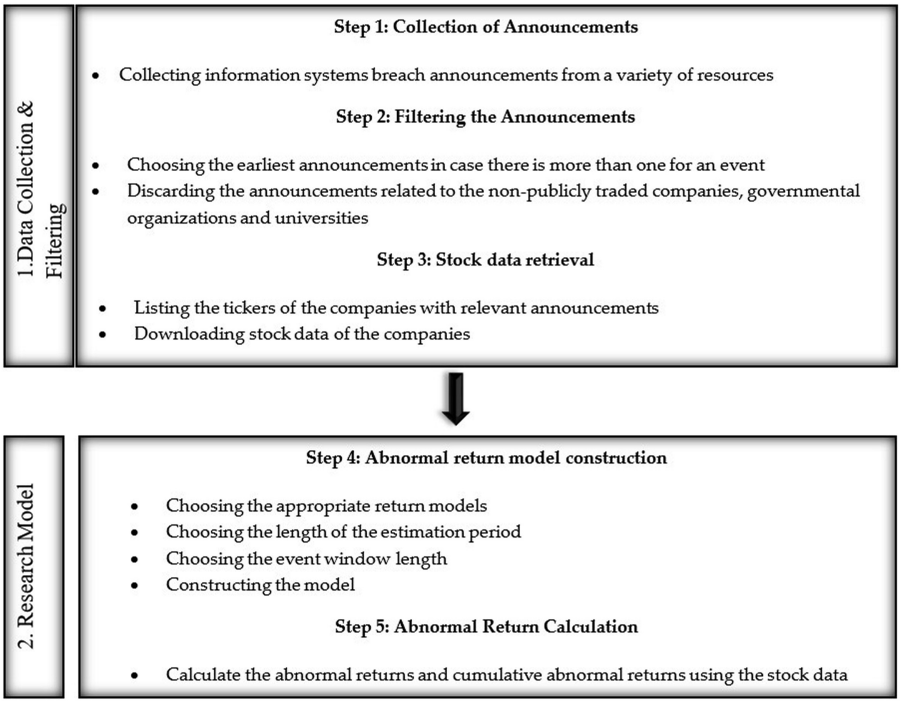

Figure 1.
Methodology of the study

"information system attack," "computer attack" and "computer system security" while searching the cybersecurity incidents reports. At the end of this step, 337 events between the years 2000–2018 are collected, all the events and the initial announcement dates are validated by the news of various major media outlets.

It is not always clear on the media when the initial announcement is made about an incident. In Step 2, for each event, several outlets are cross-checked for defining the exact event and the first announcement date. If the exact date of the initial announcement is not found, that event is discarded from the sample. In some cases, several companies were exposed to a single major attack. In those cases, each company is treated as a separate event.

For the purpose of the study, it is focused on the security breaches of publicly traded companies. Therefore, the data of the Government, Military, Academic Organizations and the data of the private companies that are not publicly listed is eliminated, which is 111 events between the years 2000 and 2018.

In Step 3, where the stock data of the related companies is collected, the study had the following limitations:

(1) Some of the companies have been acquired by other companies and the data price of the original company that faced the event at the event date is not available.

(2) Some of the companies were not publicly traded at the event date.

(3) Some of the companies were publicly traded at the event date, but after a period of time they are delisted, so the market data has been removed.

(4) The market was closed on the event date.

Due to the unavailable stock data of some companies, the sample size is reduced to 192 events between the years 2000 and 2018. The majority of incidents happened in 2006 (10.42%) and 2013 (9.38%). Also, there is no incident reported publicly in the sample for 2009. The events in the sample across the years are presented in Table 2.

The sample of companies is divided into seven groups as *Communications, Consumer Goods, Energy, Financials, Healthcare, Industrials, and Technology* sectors. The company

Table 2. Breakdown of the events by year

Year	Number of incidents	% of the sample
2018	6	3.13
2017	8	4.17
2016	6	3.13
2015	2	1.04
2014	9	4.69
2013	18	9.38
2012	7	3.65
2011	14	7.29
2010	3	1.56
2009	0	0.00
2008	7	3.65
2007	10	5.21
2006	20	10.42
2005	16	8.33
2004	12	6.25
2003	15	7.81
2002	7	3.65
2001	15	7.81
2000	17	8.85

sector information is gathered from the website of Bloomberg. Table 3 illustrates the privacy-related incidents by different sectors. The majority of the events occurred in the Communications (26.56%) and Financials sector (23.96%), followed by Consumer Goods (20.83%) and Technology (22.67%) sectors. Since the sample size of the "Energy," "Healthcare" and "Industrials" sectors were small, they are discarded from the sample.

In the following section, three models for the calculation of the abnormal stock returns and our analyses are presented.

3.2 Research model

In this study, an event study is conducted to measure the financial impact of information systems security breaches on the companies operating in 4 different sectors (Communications, Consumer Goods, Financials, and Technology).

First, the event window is selected, where the impact of the breach is observed. For a typical timeline for an event study see Figure 2, where:

$T0 - T1$ interval represents the estimation period,
$T1 - T2$ interval represents the event window,
0 represents the day of the announcement of the event,
$T2 - T3$ interval is the post-event window.

The event window is a time interval that includes $-T1$ days before and $+T2$ days after the day of the announcement. In this study, the event window is selected as 5 days prior and 10 days after ($[-5, 10]$) the event and to support the results, additional analyses are conducted for the $[-5, 0]$, $[-5, 1]$ and $[-5, 5]$ windows.

To estimate the financial impact of the events of information security breaches, first, the firm's return on the stock is calculated without the impact of the event, which is called the normal return. The normal return is estimated in a period where the event could not impact the return (in this paper, from day -250 to -30).

There are 3 different models in literature for calculating the normal return on the stock (Campbell *et al.*, 1997; Hendricks and Singhal, 1996): the market model, the market adjusted

Table 3. Distribution of the number of privacy breaches by the sector

Type of sector	Number of events	% of sample
Communications	51	26.56
Consumer goods	40	20.83
Energy	1	0.52
Financials	46	23.96
Healthcare	5	2.60
Industrials	10	5.21
Technology	39	22.67

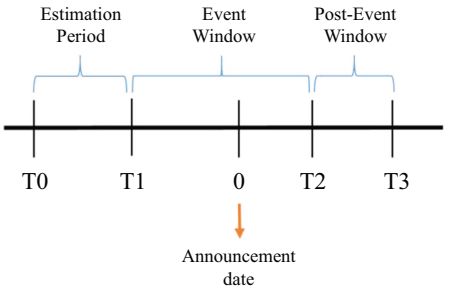

Figure 2. Timeline for the event study

model, and the mean adjusted model. The market model is most commonly used for the estimation of the expected return (MacKinlay, 1997). In this study, it is focused on the Market Model which assumes a steady linear relation between the market return and returns on the stock. Besides, the results are strengthened with the support of other models such as the Market-adjusted and Mean-adjusted models.

3.2.1 The market model. The first step of calculating the impact of the event is estimating the normal return without the impact of the event. For the estimation, the market model based on the Capital Asset Pricing Model (CAPM) is used which is a widely accepted method in the literature to estimate the stock returns (Dos Santos *et al.*, 1993):

$$Rit = ai + biRmt + eit \tag{1}$$

where

Rit represents the normal return for firm *i* on day *t*;
Rmt represents the market return on day *t*;
ai represents the intercept parameter for firm *i*;
bi is used as the slope parameter for firm *i*;
eit is random error term for the firm *i* on day *t*.

Value-weighted index depending on which market the stock of interest is traded is used as the proxy for the *Rmt* and the parameters of the market model: *ai*, *bi* and *eit* is assessed during the estimation period. The expected return estimation is based on OLS regression, which is used to estimate the regression parameters $\propto$ and β. The shortest estimation period which is commonly accepted in the literature is 120 days. For a comprehensive analysis, an estimation period starting 250 days (a full calendar year) before the announcement of the event, and ending 30 days before the announcement date (day −250 to day −30) is used in this study. The 30-day gap between the estimation period and the event window is selected to produce robust parameters as a result of the regression estimation. Following the estimation of the regression parameters, ARs are calculated for the event window (see Equation 2).

$$AR_{it} = R_{it} - \propto_i - \beta_i R_{mt} \tag{2}$$

where

i represents the event,
AR_{it} represents the abnormal security return of event *i* in period *t*,
R_{it} represents the actual return of event *i* in period *t*,
R_{it} represents the normal return for event *i* in period *t*,
$\propto$ and β are the OLS estimates,
m represents the market,
t represents the event day,
R_{mt} represents the market return in period *t*.

Following, the ARs for each event window are accumulated to obtain CARs.

3.2.2 The market adjusted model. The market-adjusted model uses only the currently available information in the event period to calculate the abnormal stock returns (Peterson, 1989). Calculation of ARs are as follows:

$$ARit = Rit - Rmt \tag{3}$$

where

i represents the event,
ARit represents the abnormal stock return of event *i* in period *t*,
Rit represents the actual return event *i* in period *t*,
Rmt represents the market return in period *t*

Following, the ARs for each event window are accumulated to obtain CARs.

3.2.3 The mean adjusted model. In the mean adjusted model, the expected returns equal to the mean security return over the estimation period (Peterson, 1989). The calculation is as follows:

$$ARit = Rit - \ Ri \tag{4}$$

where,

i represents the event,

$ARit$ represents the abnormal return of event i at time t,

Rit represents the actual return,

Ri represents the mean return on the stock during event i.

Following, the ARs for each event window are accumulated to obtain CARs.

3.2.4 Cumulative abnormal returns. There is a possibility that the available information is not reflected in the markets instantaneously; thus, there is a need for multi-day event window calculation. The abnormal returns during the event window [−5, 10] for each event window are accumulated to get CAR. The CAR for firm i for event window that begins at day $T1$ and ends at day $T2$ is:

$$\text{CAR } i\ [T1,\ T2] = \sum\nolimits_{t=T1}^{T2} \text{AR}jt \tag{5}$$

where:

$[T1,\ T2]$ = the event window,

and other terms are the same as previously.

The mean CAR is derived by averaging the CARs across all the events:

$$\overline{\text{CAR}}\ [T1,\ T2] = \frac{1}{N}\sum\nolimits_{j=1}^{N} \text{CAR}j[T1, T2] \tag{6}$$

where:

N = the number of events in the sample,

and other terms are the same as previously.

The results according to the three models (the market model, the mean adjusted model, and the market adjusted model) are presented in the next section.

4. Results and findings

An estimation window from −250 to −30 and the event window from −5 to +10 are used in the analyses. The results are tested within three models: Market Model, Market-Adjusted Model, Mean Adjusted Model. The results are presented in Table 4, based on 192 events in the sample.

Table 4 shows the values for the AR on the announcement day. Following, the accumulated ARs are calculated from day −5 to day +10 (see Table 5).

Table 5 presents the results of the CARs for the market model, the mean adjusted model, and the market adjusted model. The results for different sectors in 4 different event windows are provided to be able to compare the results. According to the results of the Market Model, the Financials sector has a significant negative impact in all of the event windows considered ([−5, 0], [−5, 1], [−5, 5], [−5, 10]). Following the Financials sector, the Technology sector experienced the most impactful significant negative impact on stock prices. The results are significant for the Technology sector, except for the [−5, 5] event window. However, it is safe to assume that the Technology sector still experiences high negative impacts. For the Consumer Goods sector, significant negative impacts are observed on the event windows [−5, 5] and [−5, 10]. Even if not in the early post-announcement days, the Consumer Goods sector

Sectors	AR on the announcement day	Market model	Market adjusted model	Mean adjusted model
Financials	Mean abnormal return	0.03%	0.03%	−0.42%
	Median abnormal return	0.08%	0.13%	−0.69%
	Percentage below zero	43.75%	43.75%	62.50%
Communications	Mean abnormal Return	0.43%	0.39%	0.18%
	Median abnormal return	0.50%	0.56%	0.17%
	Percentage below zero	37.14%	34.29%	42.86%
Consumer goods	Mean abnormal return	1.66%	1.68%	1.21%
	Median abnormal return	0.27%	0.30%	0.07%
	Percentage below zero	36.84%	36.84%	47.37%
Technology	Mean abnormal return	−0.16%	−0.19%	−0.48%
	Median abnormal return	−0.68%	−0.57%	−0.64%
	Percentage below zero	61.54%	61.54%	69.23%

Table 4. AR results for the 4 different sectors

Sector	Event window	Market model CAR	Market adjusted model CAR	Mean adjusted model CAR	Market model CAR *t*-stat	Market adjusted model CAR *t*-stat	Mean adjusted model CAR *t*-stat
Financials	[−5, 0]	−2.96%	−2.84%	−3.59%	−1.93**	−1.99***	−1.8**
	[−5, 1]	−2.70%	−2.34%	−3.39%	−1.76**	−1.64*	−1.7**
	[−5, 5]	−4.20%	−3.90%	−4.64%	−2.73***	−2.73***	−2.33***
	[−5, 10]	−5.04%	−4.70%	−6.12%	−3.28***	−3.29***	−3.08***
Technology	[−5, 0]	−1.05%	−1.44%	−1.59%	−1.62*	−2.12***	−2.14***
	[−5, 1]	−1.22%	−1.53%	−1.48%	−1.88**	−2.24***	−2***
	[−5, 5]	−0.43%	−0.92%	−1.10%	−0.67	−1.35*	−1.47*
	[−5, 10]	−1.51%	−2.09%	−2.04%	−2.33***	−3.07***	−2.74***
Communications	[−5, 0]	0.87%	0.75%	0.59%	1.6*	1.62*	2.07***
	[−5, 1]	0.48%	0.46%	0.09%	0.88	0.99	0.31
	[−5, 5]	0.29%	0.11%	−0.33%	0.53	0.25	−1.15
	[−5, 10]	1.75%	1.34%	0.30%	3.22***	2.9***	1.05
Consumer goods	[−5, 0]	0.26%	1.01%	0.43%	0.38	1.6*	0.67
	[−5, 1]	−0.20%	0.52%	−0.55%	−0.29	0.83	−0.85
	[−5, 5]	−1.33%	−0.23%	−1.65%	−1.96**	−0.37	−2.56***
	[−5, 10]	−1.86%	−0.84%	−1.99%	−2.74***	−1.32*	−3.09***

Note(s): *, ** and *** denote the significance levels 10%, 5% and 1% respectively

Table 5. Mean CARs and test statistics for the four different sectors

is experiencing a significant negative impact in the following days. Counterintuitively, no significant negative impact is observed in the Communications sector. In fact, a positive impact is observed for all the event windows. Although the positive impact cannot be correlated with the information security breach announcements, it is safe to assume that the Communication sector does not experience any negative impact from the information security breach announcements. Therefore, H1 is rejected and it is concluded that not all the sectors are experiencing significant negative financial effects after the information security breaches.

Figure 3 presents the CARs of the Consumer Goods, Financials, Technology, and Communications sectors according to the market model, market-adjusted model, and mean adjusted model.

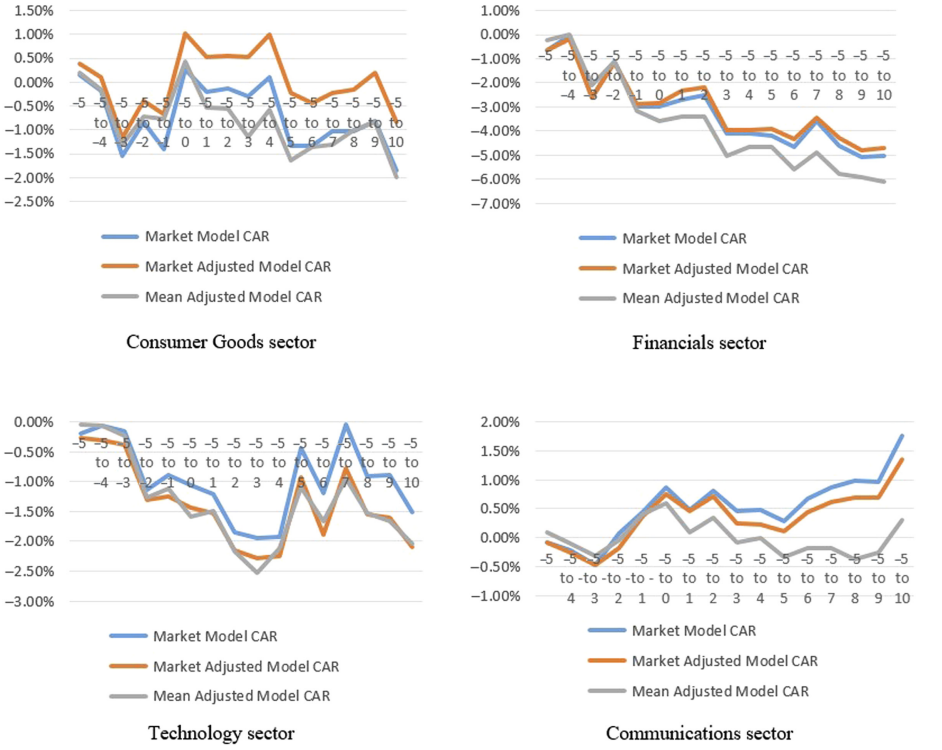

Figure 3.
Cumulative abnormal returns for consumer goods, financials, technology and communication sectors

4.1 Financials sector

The results show that the Financials sector experienced a significant negative impact on all of the event windows ([−5, 0], [−5, 1], [−5, 5], [−5, 10]) for all of the models, and it is the most financially impacted sector amongst the others. The findings our consisting with the existing literature on the financial impacts of information security breaches on the Financials sector, i.e. the negative impacts on the financial sector are greater than the impacts on the other sectors (Malhotra and Malhotra, 2011; Morse *et al.*, 2011 Arcuri *et al.*, 2017).

Interestingly, it is observed that the stock prices started to decrease before 3 days of the event and continued to decrease after day 1 (see Figure 3). Arcuri *et al.* (2017) also found a great negative financial impact on Financials sector before the cyberattack announcements. Thus, there is a possibility that the investors received the news of the event before the announcement day through insider information flow and it resulted in a pre-announcement stock price decrease.

It is assumed the investors are more prone to reflect on the information security breaches in the Financials sector because the sector possesses the most critical customer information. Due to its nature, the Financials services sector would face higher risk exposure and consequently high probable losses. Financials sector is getting attacked more than any other sector (World Bank, 2018) and companies in the sector should take necessary preventive measures against security breaches and related insider information flow, be prepared for any kind of exposure, and stay vigilant all the time.

4.2 Technology sector

Following the Financials sector, the Technology sector experienced the negative impacts of information security breach announcements severely. The results are significant for the Technology sector except for the [−5, 5] event window in the Market Model CAR. If checked with the Market Adjusted Model and Mean Adjusted model, the results are significant for the event window [−5, 5] as well. The technology sector started to face a decrease in the stock prices on day −3, with a decreasing trend until day 3 (see Figure 3). The stock return values started to fluctuate after day 4. The strong negative impact of the event on the Technology sector indicates the vitality of the information security-related activities for the Technology sector. It is assumed one of the reasons for this strong impact is because shareholders' expectations from the technology firms are higher than non-technology firms. Stakeholders are expecting high expertise in the technology in this sector and are assuming they should be capable of preventing any kind of information systems attack. Investors are likely penalizing the Technology sector more severely than the other sectors.

4.3 Consumer goods sector

The Consumer Goods sector experienced significant negative impacts on the event windows [−5, 5] and [−5, 10]. Despite the decrease in the stock prices after the announcement day (see Figure 3) in the Consumer Goods sector, the impact is not significant in the early post-announcement days. However, the negative impact becomes significant after some time.

The Consumer Goods sector has been affected by cyber breaches less than the Financials and the Technology sector, thus we assume the stakeholders are not penalizing the Consumer Goods sector businesses as severely as the technology and financial firms. It is argued that the Consumer Goods industry does not necessarily have to gain the trust of the stakeholders as the Financials and Technology sectors, and the expectations of the stakeholders are not extremely high in the Consumer Goods sector. Although the consumer goods sector was not impacted by the events as severely as the Financials and the Technology sectors, it still would benefit to take the related information security measures.

4.4 Communications sector

Counterintuitively, no significant negative impact is observed in the Communications sector. In fact, there is a positive impact on all the event windows. Due to the counterintuitive results, the results of the Market Adjusted Model CAR and Mean Adjusted Model CAR are examined in addition to the Market Model CAR. Still, the results of all of the models are consistent and none of the models in the Communication sector shows a significant negative impact.

Therefore it is concluded by stating the Communication sector did not experience any negative impact from the information security breach announcements. We assume there is already high trust in the communications sector and the sector manages the pre and post-announcement days of these kinds of events effectively. However, these analyses do not guarantee the same behavior for future events, so we enforce the recommendations about systems security for the communication sector as well.

5. Conclusions

Information systems play a major role in today's world by providing effective managerial tools for businesses. Information systems bring huge security risks and threats to all companies along with their supporting nature (D'Arcy *et al.*, 2014), and investors have increased concerns about the publicly traded companies' exposure to the cybersecurity risks (Spanos and Angelis, 2016). It is expected that companies experience negative financial

impacts of information security-related events, yet, there are still some conflicting views and mixed results in the literature (Amir, 2018).

In this paper, it is focused on the financial impact of the security-related risk events on firms' market value in 4 different sectors. Information security incidents are collected from 2000 to 2018, 192 information security breach events are analyzed using event study methodology, and statistical evidence is found about the different impacts of information systems security breach in 4 sectors, which shows the vitality of subsampling in this kind of research. The analyses on the overall sample could bring generalizable insights, however, when the sample is divided into subsamples the results are more insightful and open to discussion. However, subsampling requires a relatively big sample size and publicly traded firms are reluctant to reveal the security breach information to the market, so establishing a large sample size is challenging for this research topic. This paper contributes to the literature with a relatively large sample and cross-sector comparison between the 4 biggest impacted sectors in the sample, which are Consumer Goods, Technology, Financials, and Communications sectors. Evidence is found that the Financials sector faced the most powerful impact from the cyberthreats followed by the Technology sector. The Consumer Goods sector did not face any significant negative impact on the early post-announcement dates, however, results became significant in the later post-announcement dates ([−5, 5], [−5, 10]). It is found that the Communications sector does not experience a negative impact from the attacks. The results of the analyses show different market reactions for different sectors, the security breach impact is higher in some sectors than the others.

The results of this paper should help businesses to gain insights into the financial impacts of the information systems security events. Even the sector of the business faced a high financial impact on the market value in the past or not, investments in information systems security are vital for organizations to avoid such costs in the future. Taking preventive measures will build the confidence of the stakeholders, meet their expectations and even create a positive reputation by showing the business is vigilant all the time.

5.1 Managerial implications

The results of this paper provide evidence to managers to justify their investments in security, i.e. establishing a new department, hiring a workforce, reaching an agreement with the security service providers. Although stock prices of publicly traded firms increase or decrease over time, the event study methodology discovers a specific impact created by the occurrence of an event. How to handle this effect carefully is vital for the managers of those firms. To protect the value of a firm, maintain stability and preventing sudden value decrease in stocks, managers should handle the security risks proactively. The financial impact of information security breaches is not the same for every sector, however, there are some common measures that all the businesses could take to increase their security levels. This study can guide businesses in this effort. According to the results, the strategic insights are as follows.

All efforts for eliminating the risks should be systematic and should be carried out under the appropriate corporate governance framework and the top management team should be responsible for carrying out the cybersecurity activities throughout the company. Security breach events should be reviewed in the annual meetings along with the other key important issues. The necessary measures and paths should be decided and updated regularly. These measures should include both preventive and corrective actions if necessary. The involvement of the senior management and the proactive security measures are the most important antecedents for increasing cybersecurity in a company (Kumar *et al.*, 2020). As a benefit of a corporate governance framework and standardized security measures, all employees of the company would apply the same information security practices, and it would

safeguard the information's integrity and value until it reaches the authorized outside recipients. This kind of culture preserves and protects the asset of information (Wong *et al.*, 2020).

The increased awareness in leadership is vital to provide the companies with a chance to be ready for the possibility of the occurrence of these risks. Besides, the efforts on the management side will bring consumer confidence to those firms. Showing commitment to the digital security of the business systems will lead to an enhancement in the business activities and stock performances. Today, the awareness of the information systems issues among the public has increased, and thus they can interpret the endeavors of the organizations more effectively. Companies can benefit from this situation to create a good public perception, whether their systems are breached or not. However, adopting new information systems might create vulnerability to exposers and new types of errors. Thus, a careful new system or equipment evaluation is vital before integrating them into the operations of a firm. Likewise, the training of the employees and their supervisors for the new system or equipment will help them to handle those possible errors by following clear and effective procedures.

The cost of assuring information security creates a challenging situation. In case a company invests in cyber-security, and yet there are no security breaches over time, the management could have a perception that the company is investing more than necessary over the security initiatives. The worth of the information security investment is challenging to prove while there are no security breach events that a firm encounters, yet the top management should not forget the unseen benefits of security investments. There is a good chance of security challenges will continue to threaten the firms. For the prevention of the negative impacts of the information security risks, firms need to declare an open privacy and security policy and inform both their employees and shareholders about the rules related to sensitive security threats. Providing the necessary level of security could be costly; however, security assurance is important for the market value, thus survival of the firms.

In conclusion, the information systems' security expenditures are an investment rather than an expenditure. Firms need to spend on systems security strategically to satisfy the expectations of their stakeholders. Security breach events may cause financial losses to firms and decrease their value by the loss of reputation. Firms even may benefit from taking necessary security-related precautions. Being transparent about the new security strategies of the firm, shareholders' trust in the firm will increase which will create a positive reputation.

5.2 Theoretical implications

There is a need in the literature to examine the financial impacts of information security breaches in different sectors (Smith *et al.*, 2019; Tweneboah-Kodua *et al.*, 2018). The existing studies focusing on the sectoral impacts of the information security breaches are limited and they are mostly focused on the financial sector (Malhotra and Malhotra, 2011; Lagazio *et al.*, 2014; Arcuri *et al.*, 2017). The main contribution of this paper is that it provides evidence about the financial impacts of the information systems breaches on more sectors such as the Consumer Goods, Technology, Financials and Communications sectors separately.

Second, it highlights the financial reactions from different sectors are different and therefore suggests that different safety measures would be appropriate for different sectors. Statistical evidence is provided to managers to justify their investments in information security for these sectors and provides recommendations on how to build preventive measures to secure the market value of their firms.

5.3 Limitations of the study recommendations for the future research

The research for the economic aspects of information security breaches has similar limitations in terms of the lack of big sample size (Acquisti *et al.*, 2006; Andoh-Baidoo and

Osei-Bryson, 2007; Bose and Leung, 2013). The main reason that the researchers struggle to find a big dataset is that public firms are usually not eager for making announcements about events like security breaches. Finding the data for such negative events is not trivial if they are not reported publicly by the company. These relatively small samples also prevent the researchers from investigating the topic in more detail, e.g. dividing their data into subsections. Similarly, in this research, the "Energy," "Healthcare" and "Industrials" sectors are discarded due to their small sample size. For future research, more expanded datasets will lead to increased robustness of the findings and the research and the effects of information security breaches could be analyzed for more sectors.

Similarly, Hovav and D'Arcy (2004) stated that their sample was limited to only one type of defect, which is the effect of viruses, and they examined the effect on only one category of products, which are produced by mass production technology. There is a lack of evidence if the results are valid for the other types of defects and other types of products. Therefore, future research could focus on the announcement of various types of information security breaches, and which type of breach creates the highest negative financial impact for the businesses.

References

Acquisti, A., Friedman, A. and Telang, R. (2006), "Is there a cost to privacy breaches? An event study", *ICIS 2006 Proceedings of the International Conference on Information Systems*, pp. 1563-1580.

Alharbi, I.M., Zyngier, S. and Hodkinson, C. (2013), "Privacy by design and customers' perceived privacy and security concerns in the success of e-commerce", *Journal of Enterprise Information Management*, Vol. 26 No. 6, pp. 702-718.

Amankwah-Amoah, J. and Wang, X. (2019), "Opening editorial: contemporary business risks: an overview and new research agenda", *Journal of Business Research*, Vol. 97, pp. 208-211.

Amir, E., Levi, S. and Livne, T. (2018), "Do firms underreport information on cyber-attacks? Evidence from capital markets", *Review of Accounting Studies*, Vol. 23 No. 3, pp. 1177-1206.

Andoh-Baidoo, F.K. and Osei-Bryson, K.M. (2007), "Exploring the characteristics of Internet security breaches that impact the market value of breached firms", *Expert Systems with Applications*, Vol. 32 No. 3, pp. 703-725.

Arcuri, M.C., Brogi, M. and Gandolfi, G. (2017), "How does Cyber Crime affect firms? The effect of information security breaches on stock returns", *Proceedings of the First Italian Conference on Cybersecurity*, pp. 175-193.

Aytes, K., Byers, S. and Santhanakrishnan, M. (2006), "The economic impact of information security breaches: firm value and intraindustry effects", *AMCIS 2006 Proceedings*, pp. 3305-3312.

Bendovschi, A. (2015), "Cyber-attacks–trends, patterns and security countermeasures", *Procedia Economics and Finance*, Vol. 28, pp. 24-31.

Bolster, P., Pantalone, C.H. and Trahan, E.A. (2010), "Security breaches and firm value", *Journal of Business Valuation and Economic Loss Analysis*, Vol. 5 No. 1, pp. 1-11.

Bose, I. and Leung, A.C.M. (2013), "The impact of adoption of identity theft countermeasures on firm value", *Decision Support Systems*, Vol. 55 No. 3, pp. 753-763.

Campbell, J.Y., Lo, A.W. and MacKinlay, A.C. (1997), *The Econometrics of Financial Markets*, Princeton University Press, Princeton, NJ.

Campbell, K., Gordon, L.A., Loeb, M.P. and Zhou, L. (2003), "The economic cost of publicly announced information security breaches: empirical evidence from the stock market", *Journal of Computer Security*, Vol. 11 No. 3, pp. 431-448.

Cardenas, J., Coronado, A., Donald, A., Parra, F. and Mahmood, M.A. (2012), "The economic impact of security breaches on publicly traded corporations: an empirical investigation", *AMCIS 2012 Proceedings*, pp. 1-9.

Cavusoglu, H., Mishra, B. and Raghunathan, S. (2004), "The effect of internet security breach announcements on market value: capital market reactions for breached firms and internet security developers", *International Journal of Electronic Commerce*, Vol. 9 No. 1, pp. 70-104.

Chai, S., Kim, M. and Rao, H.R. (2011), "Firms' information security investment decisions: stock market evidence of investors' behavior", *Decision Support Systems*, Vol. 50 No. 4, pp. 651-661.

Chaterjee, D., Richardson, V.J. and Zmud, R.W. (2001), "Examining the shareholder wealth effects of announcements of newly created CIO positions", *MIS Quarterly*, Vol. 25 No. 1, pp. 43-70.

Dos Santos, B., Peffers, K. and Mauer, D. (1993), "The impact of information technology investment announcements on the market values of the firms", *Information Systems Research*, Vol. 4 No. 1, pp. 1-23.

D'Arcy, J., Herath, T. and Shoss, M.K. (2014), "Understanding employee responses to stressful information security requirements: a coping perspective", *Journal of Management Information Systems*, Vol. 31 No. 2, pp. 285-318.

Ernst and Young (2008), *Global Information Security Survey 2008*, Ernst & Young LLP, Londo.

Ettredge, M.L. and Richardson, V.J. (2003), "Information transfer among internet firms: the case of hacker attacks", *Journal of Information Systems*, Vol. 17 No. 2, pp. 71-82.

Ettredge, M., Guo, F. and Li, Y. (2018), "Trade secrets and cyber security breaches", *Journal of Accounting and Public Policy*, Vol. 37 No. 6, pp. 564-585.

Fama, E.F. (1970), "Efficient capital markets: a review of theory and empirical work", *The Journal of Finance*, Vol. 25 No. 2, pp. 383-417.

Fama, E.F. (1991), "Efficient capital markets: II", *The Journal of Finance*, Vol. 46 No. 5, pp. 1575-1617.

Gatzlaff, K.M. and McCullough, K.A. (2010), "The effect of data breaches on shareholder wealth", *Risk Management and Insurance Review*, Vol. 13 No. 1, pp. 61-83.

Goel, S. and Shawky, H.A. (2009), "Estimating the market impact of security breach announcements on firm values", *Information and Management*, Vol. 46 No. 7, pp. 404-410.

Gordon, L.A. and Loeb, M.P. (2002), "The economics of information security investment", *ACM Transactions on Information and System Security*, Vol. 5 No. 4, pp. 438-457.

Gordon, L.A., Loeb, M.P. and Sohail, T. (2003), "A framework for using insurance for cyber-risk management", *Communications of the ACM*, Vol. 46 No. 3, pp. 81-85.

Gordon, L.A., Loeb, M.P. and Zhou, L. (2011), "The impact of information security breaches: has there been a downward shift in costs?", *Journal of Computer Security*, Vol. 19 No. 1, pp. 33-56.

Hamilton Place Strategies (2015), *Cybercrime Costs More than You Think*, Washington, DC.

Harris, S. (2010), *CISSP All-In-One Exam Guide*, McGraw-Hill, New York City.

Hendricks, K.B. and Singhal, V.R. (1996), "Quality awards and the market value of the firm: an empirical investigation", *Management Science*, Vol. 42 No. 3, pp. 415-436.

Hiscox (2020), "Hiscox cyber readiness report 2020 (online)", available at: https://www.hiscox.com/sites/default/files/content/documents/2020-Hiscox-Cyber-Readiness-Report_USA.pdf (accessed 5 April 2021).

Hogan, K.M., Olson, G.T. and Angelina, M. (2020), "A comprehensive analysis of cyber data breaches and their resulting effects on shareholder wealth", available at: https://ssrn.com/abstract=3589701 or http://dx.doi.org/10.2139/ssrn.3589701.

Hovav, A. and D'Arcy, J. (2003), "The impact of denial-of-service attack announcements on the market value of firms", *Risk Management and Insurance Review*, Vol. 6 No. 2, pp. 97-121.

Hovav, A. and D'Arcy, J. (2004), "The impact of virus attack announcements on the market value of firms", *Information Systems Security*, Vol. 13 No. 3, pp. 32-40.

Jeong, C.Y., Lee, S.Y.T. and Lim, J.H. (2019), "Information security breaches and IT security investments: impacts on competitors", *Information and Management*, Vol. 56 No. 5, pp. 681-695.

Kamiya, S., Kang, J.K., Kim, J., Milidonis, A. and Stulz, R.M. (2020), "Risk management, firm reputation, and the impact of successful cyberattacks on target firms", *Journal of Financial Economics*, Vol. 139 No. 3, pp. 719-749.

Kannan, K., Rees, J. and Sridhar, S. (2007), "Market reactions to information security breach announcements: an empirical analysis", *International Journal of Electronic Commerce*, Vol. 12 No. 1, pp. 69-91.

Kumar, S., Biswas, B., Bhatia, M.S. and Dora, M. (2020), "Antecedents for enhanced level of cyber-security in organisations", *Journal of Enterprise Information Management*. doi: 10.1108/JEIM-06-2020-0240.

Kvochko, E. and Pant, R. (2015), "Why data breaches don't hurt stock prices", *Harvard Business Review*, Vol. 31, Cambridge, available at: https://hbr.org/2015/03/why-data-breaches-dont-hurt-stock-prices.

Lab, K. (2012), *Global IT Security Risks: 2012*, Moscow.

Lagazio, M., Sherif, N. and Cushman, M. (2014), "A multi-level approach to understanding the impact of Cyber Crime on the financial sector", *Computers and Security*, Vol. 45, pp. 58-74.

Landoll, D.J. (2006), *The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments*, 2nd ed., Auerbach Publications, Boca Raton, FL.

Loch, K.D., Carr, H.H. and Warkentin, M.E. (1992), "Threats to information systems: today's reality, yesterday's understanding", *MIS Quarterly*, Vol. 16 No. 2, pp. 173-186.

MacKinlay, A.C. (1997), "Event studies in economics and finance", *Journal of Economic Literature*, Vol. 35 No. 1, pp. 13-39.

Malhotra, A. and Malhotra, C.K. (2011), "Evaluating customer information breaches as service failures: an event study approach", *Journal of Service Research*, Vol. 14 No. 1, pp. 44-59.

Markoff, J. (2002), *Stung by Security Flaws, Microsoft Makes Software Safety a Top Goal*, The New York Times, New York.

McShane, M. and Nguyen, T. (2020), "Time varying effects of cyberattacks on firm value. The Geneva Papers on Risk and Insurance", *Issues and Practice*, Vol. 45 No. 4, pp. 580-615.

McWilliams, A. and Siegel, D. (1997), "Event studies in management research: theoretical and empirical issues", *Academy of Management Journal*, Vol. 40 No. 3, pp. 626-657.

Morse, E.A., Raval, V. and Wingender, J.R. Jr (2011), "Market price effects of data security breaches", *Information Security Journal: A Global Perspective*, Vol. 20 No. 6, pp. 263-273.

NIST (National Institute of Standards and Technology) (2013), *Security and Privacy Controls for Federal Information Systems and Organizations*, NIST Special Publication, Gaithersburg, Maryland, pp. 800-853.

Nishat Faisal, M., Banwet, D.K. and Shankar, R. (2007), "Information risks management in supply chains: an assessment and mitigation framework", *Journal of Enterprise Information Management*, Vol. 20 No. 6, pp. 677-699.

Peterson, P.P. (1989), "Event studies: a review of issues and methodology", *Quarterly Journal of Business and Economics*, Vol. 28 No. 3, pp. 36-66.

Pirounias, S., Mermigas, D. and 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*, Vol. 19 No. 4, pp. 257-271.

Richardson, R. (2008), *CSI Computer Crime and Security Survey*, Computer Security Institute, San Francisco, CA.

Richardson, V.J., Smith, R.E. and Watson, M.W. (2019), "Much ado about nothing: the (lack of) economic impact of data privacy breaches", *Journal of Information Systems*, Vol. 33 No. 3, pp. 227-265.

Schuurman, R. (2019), "The effects of data breaches on the stock price in the period 2016-2018", Bachelor Thesis of Economics and Business Economics, Erasmus University Rotterdam, Rotterdam.

SEC (2018), "Commission statement and guidance on public company cybersecurity disclosures", available at: https://www.sec.gov/rules/interp/2018/33-10459.pdf.

Smith, K.T., Jones, A., Johnson, L. and Smith, L.M. (2019), "Examination of cybercrime and its effects on corporate stock value", *Journal of Information, Communication and Ethics in Society*, Vol. 17 No. 1, pp. 42-60.

Solon, O. (2018), "Facebook faces $1.6bn fine and formal investigation over massive data breach", *The Guardian News*, available at: https://www.theguardian.com/technology/2018/oct/03/facebook-data-breach-latest-fine-investigation (accessed 5 April 2021).

Spanos, G. and Angelis, L. (2016), "The impact of information security events to the stock market: a systematic literature review", *Computers and Security*, Vol. 58, pp. 216-229.

Sun, L., Srivastava, R.P. and Mock, T.J. (2006), "An information systems security risk assessment model under the Dempster-Shafer theory of belief functions", *Journal of Management Information Systems*, Vol. 22 No. 4, pp. 109-142.

Tanimura, J.K. and Wehrly, E.W. (2015), "The market value and reputational effects from lost confidential information", *International Journal of Financial Management*, Vol. 5 No. 4, pp. 8-35.

Tweneboah-Kodua, S., Atsu, F. and Buchanan, W. (2018), "Impact of cyberattacks on stock performance: a comparative study", *Information and Computer Security*, Vol. 26 No. 5, pp. 637-652.

Wong, W.-P., Tan, K.H., Chuah, S.H.-W., Tseng, M.-L., Wong, K.Y. and Ahmad, S. (2020), "Information sharing and the bane of information leakage: a multigroup analysis of contract versus noncontract", *Journal of Enterprise Information Management*, Vol. 34 No. 1, pp. 28-53, doi: 10.1108/JEIM-11-2019-0368.

World Bank (2018), "Financial sector's cybersecurity: regulations and supervision", available at: http://documents.worldbank.org/curated/en/686891519282121021/pdf/123655-REVISED-PUBLCFinancial- Sectors-Cybersecurity-Final-LowRes.pdf.

World Economic Forum (2020), "The global risks report 2020 (online)", available at: https://www.weforum.org/reports/the-global-risks-report-2020 (accessed 5 April 2021).

Yayla, A.A. and Hu, Q. (2011), "The impact of information security events on the stock value of firms: the effect of contingency factors", *Journal of Information Technology*, Vol. 26 No. 1, pp. 60-77.

Corresponding author
Cansu Tayaksi can be contacted at: ctayaksi@mit.edu