




Article

The Long-Run Impact of Information Security Breach Announcements on Investors' Confidence: The Context of Efficient Market Hypothesis

Syed Emad Azhar Ali ^{1,*}, Fong-Woon Lai ¹, Rohail Hassan ^{2,*} and Muhammad Kashif Shad ¹

¹ Department of Management & Humanities, Univeristi Teknologi PETRONAS, Seri Iskandar 32610, Malaysia; laifongwoon@utp.edu.my (F.-W.L.); mkashifshad@gmail.com (M.K.S.)

² Othman Yeop Abdullah Graduate School of Business (OYAGSB), Universiti Utara Malaysia, Kuala Lumpur 50300, Malaysia

* Correspondence: emadazhar2018@gmail.com (S.E.A.A.); rohail.hassan@uum.edu.my (R.H.)

Abstract: Information and communication technologies (ICTs) are the cornerstone for sustainable development, but if they are not appropriately managed, they will impede progress towards the United Nations Global Sustainable Development Goals. Among undesirable impacts, emphasis must be put on the risk of information security (ISec) breaches, as they pose a potential threat to businesses there. Especially for publicly traded firms, they could create a long-lasting influence on their financial performance and, thus, stock investors' confidence. Following the efficient market hypothesis's footsteps, previous studies have examined only the short-run impact on investors' confidence ensuing to ISec breach announcements. Therefore, this study investigates the long-run impact of ISec breach announcements on investors' confidence. Based on a sample of 73 ISec breach announcements during 2011–2019, this paper examines the impact on investors' confidence, as demonstrated by long-run abnormal returns and equity risk of those firms. Using a one-to-one matched sampling approach, each firm's performance is analyzed with its control firm over eighteen months, starting six months before the announcement, through twelve months after the announcement. Firms experienced a significant negative abnormal return of 15% to 18% during the twelve months following the breach announcement. In comparison, equity risk increased by 11% within six months before and after an announcement. This study can help investors, managers, and researchers better understand a long-term relationship between ISec breaches and investor confidence in the context of efficient market hypothesis.



Citation: Ali, S.E.A.; Lai, F.-W.; Hassan, R.; Shad, M.K. The Long-Run Impact of Information Security Breach Announcements on Investors' Confidence: The Context of Efficient Market Hypothesis. *Sustainability* **2021**, *13*, 1066. <https://doi.org/10.3390/su13031066>

Academic Editor: Carlos Rodríguez Monroy
Received: 11 November 2020
Accepted: 11 December 2020
Published: 21 January 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

Keywords: efficient market hypotheses; long-run abnormal returns; equity risk; Sustainable Development Goals (SDGs)

1. Introduction

In an attempt to accomplish many of the Sustainable Development Goals (SDGs) adopted by the United Nations General Assembly in September 2015, as SDG 9 (“Industry, Innovation and Infrastructure Development”) and SDG 17 (“Revitalize the Global Partnership for Sustainable Development”), the adoption and development of information and communication technologies (ICTs) is essential for businesses and, from a macro-economic perspective, is crucial. Indeed, ICTs can link individuals and organizations, encourage inclusive and sustainable industrialization, facilitate knowledge sharing and creativity across sectors [1–4]. Hence, digitalization is gradually being demonstrated as a crucial element for sustainable development for these reasons [5,6].

Safety and security are crucial within cyberspace for innovations to deliver their developmental impact effectively. In other words, ICTs can accomplish the 2030 SDGs of the United Nations, but at the expense of information security (ISec) risk management [2,3,7].

A Harvard's business review defines ISec breach as "an event in which important, secure or confidential data is accessed [8], manipulated or used by a nonauthorized person [9]". The victimized company has to deal with losses (e.g., loss of reputation and trust) and various litigations. Illegally accessing passwords, the manipulation of data, the shutdown of computer facilities, modification, and stealing of computer software are examples of breaches of data and violation. According to a global survey report by Ponemon [10], the number of security breaches suffered by firms has increased gradually from an average of 130 breaches in 2017 to 145 breaches in 2019.

1.1. Impact on Investors' Confidence

A firm that suffers an ISec breach will have to bear the tangible and intangible costs after such an event [11–13]. Tangible costs are the costs for labor, material, and services incurred in fixing the damage to information assets and failure to earn extra profits. In comparison, intangible costs incorporate the loss of trust and confidence of business stakeholders, including the investors in the stock market. Measuring such an effect on investors' confidence is a challenging task. Therefore, various studies have measured the loss in investor's confidence using theory for Efficient Markets [11,14–20]. In most of these studies, the negative impact was witnessed on investors' confidence manifested by negative abnormal returns. These studies were underpinned by the "Semistrong Efficient Market Hypothesis" (EMH) [21,22], according to which stock prices adjust quickly to all new information. Accordingly, the short-run examination of the ISec breach event has been performed in these studies by analyzing the stock price behavior (i.e., from few days before an event to few days after an event), exhibiting an immediate analysis of investors' confidence. While the short-run analysis helps get the market's quick reaction to an event announcement, it is imperative to explore the long-run analysis to estimate a more realistic economic impact of a breach announcement. Studies addressing this problem are unclear whether an ISec breach will affect the long-run confidence of investors.

1.1.1. Long-Run Impact on Investors' Confidence

According to the Global Cost of Data Breach Report [10], the time to identify and contain a data breach has been continuously increasing, from 257 days in 2017 to 280 days in 2020, with estimated response costs ranging around \$1 million for each firm. The announcements such as ISec breaches indicate that the firms are reluctant to disclose complete details of a breach on their first announcement. In recent times, we have witnessed events of ISec breaches where the details concerning a breach are disclosed months after the first breach announcement. For instance, in July 2019, Equifax was penalized with US\$ 700 million by the Federal Trade Commission and Consumer Financial Protection Bureau, ensuring an enormous data breach in 2017. From the investors' perspective, they will probably have a close watch on subsequent disclosures and announcements by the firm concerning an ISec breach announcement that can influence their investment decision making. Hence, an ISec-event's impact, especially concerning investors' confidence, cannot be judged only by analyzing the announcement effect. Especially in cases where the announcement and economic impact vary.

Second, market efficiency hypothesizes that the stock price movement ensuing to the announcement of an event will not be abnormal. Nevertheless, as per the studies on the revamped shape of EMH, the impact of new information on the stock market is not fully exhibited at the time of announcement [23]. Few studies have suggested that a declaration of an event would result in a slow shift in the share price and subsequent abnormal returns. Although there is an extensive argument concerning the methodology [23,24], it is vital to estimate the post-announcement abnormality to analyze a more wide-ranging impact of an event.

Considering the above arguments, probably, the abnormal effect of the ISec breach announcement by a listed firm can have a meaningful impression on future cash flows, the required rate of return, financial distress, and credit rating. All these concerns will be

manifested in investors' confidence in the long run as well. Overall, it can be hypothesized that the ISec breach announcement might lead to abnormality in long-run indicators of investors' confidence in the stock market, such as long-run abnormal returns and the equity risk. To the best of our knowledge, the literature did not discuss the long-term effect on investors' confidence following an ISec breach.

1.1.2. Impact on Long-Run Abnormal Returns

Examining the stock price behavior and subsequent stock returns is one of the proxies for investors' confidence is crucial because they reflect current, expected future costs and risks associated with a particular ISec-event from the investor's perspective [25]. It is also crucial to the affected firm's management teams because stock price reflects the firm value, which indicates the overall strength and health of a company. These factors are critical in determining factors such as the firm's future cost of capital, credit ratings, employees' and manager's compensation, management team's firing decision. Most importantly, publicly traded companies' management teams are hired to represent the owners, who are the shareholders. Hence, an increase (decrease) in share price often indicates the increasing (decreasing) investors' confidence in the firm's future cash flows.

1.1.3. Impact on Equity Risk

Another proxy for investors' confidence has been the firms' equity risk as an announcement of an ISec breach might influence it. After such an unfavorable announcement, stock price changes might result from an abnormality in forecasted risk or volatility in future cash flows [26]. Thus, change in future cash flow expectations can affect the overall equity risk of the firm. As per the author's best knowledge, previous studies have yet to explore ISec breaches' impact on equity risk.

Understanding the impact of ISec breaches on equity risk is noteworthy because adjustments in equity risk expectations can meaningfully affect the firm and its stakeholders, especially the investors [27,28]. Consequently, investors may expect a higher return, which can augment the firms' cost of capital and lowers the appeal of firms' equity. There will be higher financial distress costs and lowered ratings from credit rating agencies with a higher capital cost. Hence, equity risk changes have wide-ranging economic consequences; it is vital to comprehend the impact of ISec breaches on equity risk. This article uses equity volatility to measure the overall firm risk, calculated as the standard deviation of equity returns. Equity volatility is a widely used business risk measure by academics and practitioners alike.

Considering the alarming rise of ISec breach incidents, ISec breach announcements are expected to create a long-run negative influence on investors' confidence in a listed firm. An unfavorable abnormality might manifest that influence in its long-run stock returns and equity risk (stock volatility). Thus, the research question of this study will be as follows: What is the long-run impact of the ISec breach announcement on investors' confidence?

Likewise, the study aims to achieve the following research objectives (RO):

RO₁: *To evaluate the long-run impact of ISec breach announcements on abnormal returns of breached firms.*

RO₂: *To evaluate the long-run impact of ISec breach announcements on the equity risk of breached firms.*

The next section reviews the literature on the influence of ISec breach on investor confidence and why it is imperative to study both the long-run stock price effects and the firms' equity risk. Section 2 also highlights the theoretical foundations underpinning this research. Based on that, Section 3 exhibits the development of the hypothesis and conceptual framework of this study. Section 4 describes the methodology for forecasting the long-run confidence of investors. Section 5 presents the long-run impact of investors' confidence, as demonstrated by long-run abnormal returns and equity risk. Whereas the theoretical and practical implications of this study will be encapsulated in Section 6 along with limitations and future research opportunities in this domain.

2. Literature Review

One priority issue concerning information events has emerged in the wake of more pervasive Internet technology: How can organizations effectively measure the damages from breaches in ISec? Several extensive private sector reports, such as the Computer Security Institute/Federal Bureau for Inquiry (CSI/FBI) and Computer Emergency Response Team (CERT), have been available. However, they have not investigated the incident's influence on the financial structure of a firm. Furthermore, many companies tend to reveal incident information because reporting by the media of their flaws in ISec would lead to customer complaints and overreactions.

An influential research group has discussed various issues relating to ISec risks, such as ISec investments [29,30], institutional stimulus on innovation, and security [31]. Another research line focuses on the market implications of disclosures linked to ISec [32,33] and ISec breaches [17,32–38] by having an underpinning of “efficient market theory” and the methodology of an event study.

2.1. Efficient Market Theory and Studies on Short-Run Impact

It is not easy to gather incident data and address the standardized way of measuring its impact. Such phenomena were traditionally explored through the methodology of event studies in previous research. This methodology has been well established in finance, accounting, and management. It offers a statistical mechanism to assess an efficient market hypothesis by tracking and evaluating significant stock value changes in the post-announcement period. Likewise, in information systems (IS) fields, event studies are now a proven instrument for studying the market responses to numerous IT-related events, such as IT expansion, electronic commerce ventures, or creating a new organizational position as a Chief Information Officer (CIO). As ISec is becoming more critical to organizations, the methodology for event research has also become a useful technique for assessing security incidents' influence on firm values and investors' confidence. Studies have employed this methodology to investigate favorable ISec-events, such as IT security investment announcements by firms [39] and ISec certification [36], as well as unfavorable security events such as a denial of service (DoS) attack [11,17,40,41] virus attacks [42] and software vendor vulnerability announcements [43]. While some researchers have explored the impact on breached firms' stock returns in the light of various types of ISec breaches [11,16,42,44]. Our research may only concentrate on one sort of incident: data misuse involving illegal information access. Even though some studies are conducted to explore the effect of ISec breaches on firm value, the outcomes were inconclusive together.

For instance, a significant negative abnormal return of -3.8% was observed by Reference [45], using a three-day event window when they analyzed the stock return of 22 breach events between 1999 and 2002. Research by Reference [15] indicates a substantial adverse market reaction to a sample of 43 events between 1995 and 2000. Their analysis was based on a two-day event window, following ISec breaches involving unauthorized access to sensitive information. However, they also confirmed that the breaches did not cause a significant market response if the breach did not involve the compromise of confidential information.

A statistically significant abnormal return of -2.1% with two-day event windows [11] of 66 breaches from the 1996–2001 study was reported. Reference [46] finds an abnormal return of -0.4 percent, but still statistically meaningful at day zero, for a study of 79 breaches from 2000 to March 2006. An analysis by Reference [47] reveals statistically significant abnormal returns of -0.23% in the one-day event window of 152 breach samples from 117 firms between 2000 and 2007. Their research also reveals that the magnitude of negative abnormal returns will be higher if the breach involves a compromise of employees' data rather than clients' data. The study by Reference [48] of the six data thefts between 2011 and 2012 revealed that the compromised firm's share price had decreased significantly. They recorded that the negative yields are seen on a ten-day event window.

Although the studies mentioned above recorded significant adverse outcomes, other studies have argued differently. For example, Reference [17] studied 72 firms that have

suffered confidential information breaches from 1997 to 2003 and found statistically insignificant results during an announcement window $(-1, 2)$. Likewise, in Reference [49], an analysis of 58 ISec breach incidents between 1994 and 2006 found statistically negligible findings for a one-day to five-day incident duration.

Among all event studies on ISec, the current paper is compatible with those scholarly works which have inspected the impact of the ISec breach on the stock market. Table 1 depicts the list of those studies and the time frame, event size, event window, model used, and the main findings. It can be elucidated from most of the studies that the ISec breach will have a significant unfavorable influence on the confidence of investors as signaled by negative abnormal returns within one or two days of the breach announcement.

All these systematic research works have based only on the short-run impacts of breaches while only anecdotally exploring the long-run implications of ISec breaches. For instance, Reference [50] investigates the element of insider trading, ensuing to an announcement of ISec breach by employing a 41-day event window, which covers 258 ISec breaches. Even though they have reported a negative -1.44% stock losses, the time-span used was relatively short for representing firms' long-run market value.

2.2. Studies on Long-Run Impact

It is essential to understand first the significance of long-lasting influence before investigating the impact of ISec breach on a firm's long-run market value. As stated, the methodology of event study has been extensively used in the finance literature. It has been widely used to research how mergers, acquisitions, stock splits confront firms. All these activities demand a firm's long-run appraisal. For instance, stock returns' long-run performance after the merger and acquisition was investigated by References [51–54]. Among these studies, Reference [51] observed an abnormal 10 percent negative returns over the five years after the merger. References [55–59] used the event study methodology to analyze the influence on the long-run valuation of the firm of the dividend policy occurrence. The long-run impact of the dividend payment on the share price of a company has been studied by References [55,59] with a long-run view of one to three years. The study by Reference [59] used the one-to-three-year long-run Buy-and-Hold Abnormal Returns (BHARs) model to examine the long-run effect on the firm's stock price of corporate dividends and dis-issue announcement incidents. Research by Reference [56] analyzed treasury implementation announcements and recorded an average long-run abnormal return of 12.1 percent over a four-year study period. The event study methodology has also been employed to analyze the long-run outcome on the business market value of initial offerings and capital increases [60–64]. Among these, Reference [61] advocates that the effect of stock listing on the market values of the United States (US) firms were studied one to three years after the declaration of the event.

Table 1. Summary of previous studies.

Authors	Time Interval	Estimation Model	Sample Events	Event Window	Findings
Garg, Curtis, and Halper (2003) [45]	1996–2002	One factor	22	(0, 2)	Significant negative, (5.6%)
Campbell, Gordon, Loeb, and Zhou (2003) [15]	1995–2001	One factor	43	(−1, 1)	Insignificant negative
Hovav and D’Arcy (2003) [44]	1998–2002	One factor	23	(−1, 0), (−1, 1), (1, 5), (−1, 10), (−1, 25)	Insignificant negative
Ettredge and Richardson (2003) [14]	2000	One factor	4	(0.3), (0,6)	Significant negative, (−4 to −10%)
Cavusoglu, Mishra, and Raghunathan (2004) [8]	1996–2001	One factor	66	(0, 1)	Significant negative, (−2.1%)
Hovav and D’Arcy (2004) [16]	1988–2002	One factor	186	(0, 0), (0, 1), (0, 5), (0, 10), (0, 25)	Insignificant negative
Hovav and D’Arcy (2005) [35]	1988–2002	One factor	92	(0, 1), (0, 5), (0, 10), (0, 25)	Insignificant negative
Acquisti, Friedman, and Telang (2006) [46]	2000–2006	One factor	79	(0, 1)	Significant negative, (−0.58%)
Kannan, Rees, and Sridhar (2007) [17]	1997–2003	One factor	72	(−1, 2), (−1, 7), (−1, 29)	Insignificant negative
Goel and Shawky (2009) [40]	2004–2008	Three factor	168	(−119, 10)	Significant negative, (−1.1%)
Muntermann and Roßnagel (2009) [65]	2001–2007	One factor	97	(−5, 5)	Significant negative, (−0.42%)
Liginlal, Sim, and Khansa (2009) [66]	2005–2008	One factor	151	(−2, 9)	Significant negative, (−0.59 to −0.72%)
Gatzlaff and McCullough (2010) [67]	2004–2006	One factor	77	(0, 1)	Significant negative, (−0.46%)
Patel (2010) [68]	–	One factor	34	(0, 2), (0, 7), (0, 29)	Significant negative, (−2.27%)
Bolster, Pantalone, and Trahan (2010) [69]	2000–2007	One factor	93	(−1, 0), (−1, 1), (1, 30)	Insignificant positive

Table 1. Cont.

Authors	Time Interval	Estimation Model	Sample Events	Event Window	Findings
Andoh-Baidoo, Amoako-Gyampah, and Osei-Bryson (2010) [70]	1997–2003	One factor	41	(−1, 1)	Significant negative (3.18%)
Yayla and Hu (2011) [49]	1994–2006	One factor	123	(−1, 1), (−1, 5), (−1,10)	Significant negative, (−0.92 to −1.61%)
Katherine T. Smith, Smith, and Smith (2011) [71]	2000–2005	One factor	10	(0, 1), (0, 3)	Significant negative, (−2.2 to 3.5%)
Morse, Raval, and Wingender (2011) [72]	2000–2010	One factor	306	(0, 1)	Significant negative, (−0.28%)
Gordon, Loeb, and Zhou (2011) [73]	1995–2007	One factor, three-factor	121	(−1, 1)	Significant negative, (−1.36%)
Malhotra and Kubowicz Malhotra (2011) [18]	2000–2007	Four factor	93	(−1, 1), (2, 30)	Significant negative, (−0.78 to −1.92%)
Sinanaj and Muntermann (2013) [15]	2004–2011	One factor	72	(−5, 5)	Significant negative, (0.72 to 1.55%)
Wang, Ulmer, and Kannan (2013) [74]	1997–2008	One factor	89	(−1, 1)	Significant negative, (−0.15%)
Goel and Shawky (2014) [75]	2001–2008	One factor, four factor model	201	(−30, 30)	Significant negative, (−0.63%)
Pirounias, Mermigas, and Patsakis(2014) [76]	2008–2012	Three factor model	105	(−1, 0, 1)	Significant negative, (−0.39%)
Arcuri, Brogi, and Gandolfi (2014) [77]	1995–2012	One factor	128	(−20, 20), (−10, 10), (−5, 5), (−3, 3), (−1, 1)	Significant negative, (−0.3 to −1.2%)
Das, Mukhopadhyay, and Anand (2014) [78]	2000–2012	Three factor	101	(−1, 1), (−1, 3)	Insignificant negative
S. Modi, M. Wiles and S. Mishra Modi, Wiles, and Mishra (2015) [79]	1995–2012	One factor	128	(−2, 2)	Significant negative, (−1.17%)
Hinz, Nofer, Schiereck, and Trillig (2015) [48]	2011–2012	One factor	6	(0, 1), (0, 2), (0, 3), (0, 5)	Significant negative, (−1.16 to −4.06%)

Table 1. Cont.

Authors	Time Interval	Estimation Model	Sample Events	Event Window	Findings
Schatz and Bashroush (2016) [80]	2005–2014	One factor	120	(−1, 1), (0, 0), (1, 5), (−1, 5)	Insignificant negative
Y. Chen, Dong, Chen, and Xu (2016) [81]	2005–2014	One factor	50	(−2, 2)	Significant negative, (−2.38%)
Martin, Borah, and Palmatier (2016) [82]	2006–2015	One factor	414	(−1, 1)	Significant negative, (−0.29%)
Sinanaj and Zafar (2016) [83]	2011–2013	One factor	28	(−1, 10)	Insignificant negative
Arcuri, Brogi, and Gandolfi (2017) [84]	1995–2015	One factor	226	(−20, 20), (−10, 10), (−5, 5), (−3, 3), (−20, −1), (−10, −1), (−5, −1), (−3, −1), (0, 20), (0, 10), (0, 5), (0, 3), (0, 1)	Significant negative, (−3.32 to −0.23%)
Johnson, Kang, and Lawson (2017) [85]	2005–2014	One factor	467	(0, 2)	Significant negative, (−0.37%)
Abhishta, Joosten, and Nieuwenhuis (2017) [86]	2010–2015	Three factor	35	(−1, 0), (−1, 1), (−1, 3), (−1, 5), (−1, 10)	Insignificant negative
Rosati et al. (2017) [87]	2005–2014	Bid ask model	74	(−5, 5)	Significant negative, (−2.53%)
Hovav, Han, and Kim (2017) [88]	2001–2011	One factor	105	(−1, 0), (−1, 1), (−1, 5), (−1, 10), (−1, 25)	Significant negative, (−0.34 to −0.39%)
Patsakis, Charemis, Papageorgiou, Mermigas, and Pirounias (2018) [89]	2013–2015	One factor, Three factor	80	(0, 3)	Insignificant negative
Tweneboah-Kodua, Atsu, and Buchanan (2018) [20]	2013–2017	One factor	96	(−30, 30)	Insignificant negative
Katherine Taken Smith, Jones, Johnson, and Smith (2019) [12]	–	One factor	10	(−1, 1), (−3, 3), (−7, 7)	Insignificant negative

Table 1. Cont.

Authors	Time Interval	Estimation Model	Sample Events	Event Window	Findings
Jeong, Lee, and Lim (2019) [90]	2010–2017	One factor	118	(−2, 2), (−1, 1), (0, 1), (0, 2)	Significant negative, (−0.251 to 0.42%)
Rosati, Deeney, Cummins, van der Werff, and Lynn (2019) [91]	2011–2014	One factor	87	(0, 1), (0, 2), (0, 3), (4, 10)	Significant negative, (−0.8 to −1.6%)
Chang (2020) [92]	2003–2015	One factor, Three factor, BHAR	47, 33, and 26	(0, 0), (0, 1), (1 year), (2 years), (3 years)	Significant negative, (−0.23%)— short-run Significant negative, (−10 to −34%) —long-run

BHAR, Buy-and-Hold Abnormal Return.

The review of existing works reveals that the implications of events for the firm's long-run prospects, especially investors' confidence, have become a common concern for researchers. Long-run effects have been mostly explored with the BHAR model, one to three years after the incident. Within the information management avenue, the BHAR model was used to address the long-run value of the company about the impact of Capability Maturity Model [93], Enterprise Resource Planning, Supply Chain Management, and Customer Relationship Management [94,95]. As far as we know, the impact of an ISec breach on the company's long-run market value has not yet been researched in the avenue of ISec. This research is foremost to investigate the effects of the ISec breach on the investor's confidence in the long-run. Consequently, it is of great significance to conduct empirical research in this regard.

The term "long-run investors' confidence" itself is a function of the "long-run market value", which is the degree of change in stock price from one to three years after the event. Investors' confidence is a function of the scenarios prevalent around an event announcement, lasting for some time after an event [96]. Likewise, the event of an ISec breach can have a long-lasting impact on the firm's financials and, eventually, investors' confidence. However, most scholars have narrowed their findings to a short-run impact of ISec breach on investors' confidence.

To the author's best knowledge, a recent study by Reference [92] has been the only study that has addressed the long-run impact on investors' confidence ensuing to ISec breach. In their study, breached firm's market performance was analyzed over one to three years by employing a traditional Buy-and-Hold Abnormal Returns (BHARs) model. Using a sample of 84 firms, they have concluded that the breached firm's market performance, as proxied by long-run abnormal returns, will be negatively influenced by 10% over one year after the breach announcement. Despite being the pioneer study investigating the long-run impact of ISec breach on investors' confidence, their study was not without limitations. First, they have used the traditional event study methodology by comparing the breached firms' performance to that of the market. According to References [97,98], event study methodology makes it impossible to assess the true importance of reported abnormal returns, both in terms of the total economic effect and the test statistics. The prevalence of cross-sectional dependency is the key cause of misspecification since sample firms usually have a time-limit overlapping in long-run market prices. Cross-sectional dependency (positive or negative) contributes to skewed test results. The latest simulations show that one-to-one matching of abnormal returns produces well-specific tests [97,99,100]. According to the one-to-one matching approach, each sample firm's performance is similar to that of a similar matching firm with similar size and prior performance.

Therefore, the present study has employed a more robust and reliable methodology of one-to-one-matched-sampling to examine long-run abnormal returns for such events. Furthermore, this study also examines the impact of ISec breach on another indicator of investor confidence that is "equity risk". The existence of abnormal returns annexed with ISec breaches results from a shift in investors' expectations concerning the future cash flows of a firm that might become volatile, thereby raising the equity risk. Studies investigated how ISec-events influences the confidence of investors, and thus the cash flows of companies. The literature did not answer the effect of ISec violations on equity risk in the best of our knowledge.

3. Hypothesis Development and Conceptual Framework

The previous chapter elaborates in detail the empirical literature concerning this study, along with a theoretical framework. Based on that discussion, the current section will formulate the hypothesis and conceptual framework for this study.

3.1. ISec Breaches and Long-Run Abnormal Returns

The current study examines ISec breaches, which were publicly disclosed by the breached firms. In some cases, it was revealed that firms were announcing the ISec

breaches along with earnings announcements. Thus, giving an expression that firms delay such announcements or reluctant to disclose such information more precisely. There could be several factors behind this firm's behavior. First, firms want to control the panic and uncertainty among stakeholders, which is generally created in such situations and can eventually affect the performance of those not affected by a breach. Second, the remedial action after a breach might have already been taken by a firm, and thus there might be no urgency to announce the breach. Third, the firms might want to prohibit their competitors from any significant gain amid the post-breach scenario. Hence, other than the commission's regulatory requirement, there might not be any compulsive need to announce the ISec breach as soon as it occurs.

Despite breached firms' intention to delay the announcement, there could be signs by which ISec breaches can somewhat be anticipated, for example, the firm's webpage might become inaccessible for their customers and other stakeholders, a sluggish Internet browsing, customers might face access issues on the firm's website, pointless popping up of messages at the time of customer's log-in, abrupt changes to system passwords or accounts, and browser warning of errors. Moreover, the concerned users might face infection alarms through antivirus toolkits installed in their systems. Thus, these signals of system malfunction can negatively influence the trust and confidence of customers. Likewise, investors' confidence in the stock market might be influenced, and they might have allocated a likelihood of an ISec breach for the concerned firm. It is also probable that an ISec breach's financial impact might have already incorporated by investors in their stock returns even before the actual ISec breach announcement. Hence, the following can be hypothesized:

Hypothesis 1a (H_{1a}). *In the period before the announcement, abnormal returns of ISec breached firms will be negative.*

As regards the pre-announcement period that should be analyzed, the literature has provided limited guidance in this regard. Despite the firms' incentive to postpone the ISec breach's announcement, excessive postponement can influence the firms' credibility and lead to a possible lawsuit from investors. Considering this scenario, we analyzed the six months' pre-announcement stock returns of breached firms.

To fully evaluate the financial influence of ISec breaches, it is also vital to analyze stock price behavior in the post-announce era. Recent studies have also reported statistically unusual long-run stock price reaction ensuing to an event's announcement. Examples include repurchase offers, spin-offs, initiations and omissions on dividends, open market repurchases, stock splits, seasoned equity offerings, shareholder fights, and initial public bidding (see Reference [23] for all such studies).

There is an increasing number of studies showing a slow stock market reaction to new information, a valid reason to study the impact of ISec breaches on stocks in the post-announcement era. ISec breaches can also impact firm financials even after the announcement as consumers and suppliers respond to ISec breaches. Parallel to that, firms are also expected to take remedial measures to resolve ISec breaches. Based on these measures' success, firms might recover from these real losses due to ISec breaches or prevent any of the expected losses. Since these impacts must be part of the quantification of the overall economic impact of ISec breaches, stock returns should be measured over extended timelines ensuing to an announcement. Accordingly, there are equal possibilities of positive and negative returns in the post-announcement period. Our second hypothesis is as follows:

Hypothesis 1b (H_{1b}). *In the period after the announcement, abnormal returns of ISec breached firms will be negative.*

As has been the situation with modest expectations, the literature offers no guidance on the optimal time frame for evaluating the post announcements stock returns. The

literature has time frames ranging from one to five years. The appropriate timeframe to examine is a function of the event being studied and scholars' lucid preference. After an ISec breach disclosure, we examine stock returns over one year comprising of two intervals of six months each. This will identify the negative effects of ISec breaches and any positive effects due to remedial measures. In general, we analyze the output of stock prices at every six-month interval, starting six months before the announcement through a one year after the announcement.

3.2. ISec Breaches and the Equity Risk of the Firm

Another critical matter delved into in this study was the influence of ISec breaches on the firm's risk. Numerous authors have analyzed corporate events' effect on risk by concentrating on equity risk (volatility), as calculated by the standard deviation in the return percentage of the firm's equity, σ_e [101–104]. Nevertheless, the literature has limited evidence on the impact of ISec-events on equity volatility. It is startling because equity volatility for many of the stakeholders is a standard measure of value.

According to traditional asset price theory, equity risk is bifurcated into unsystematic and systematic volatility. It is contended that unsystematic volatility can be minimized and will not impact the capital cost. However, both types of volatilities need to be considered. The first reason is that equity volatility is predicted by a range of theoretical models concerning anticipated stock returns [105,106]. Unsystematic volatility is a risk factor that could affect capital costs, as References [107,108] show; however, Reference [109] argues this claim. Second, a significant portion of a firm's investment cannot be diversified; therefore, managers worry about unsystematic volatility, and this concern can be expressed in their decisions. Third, unsystematic volatility is essential because equity volatility depends on the option's price for a specific stock. Considering the above, this study's secondary emphasis is to evaluate ISec breaches' relationship on overall equity volatility.

Given the significant economic implications of shifts in equity volatility, understanding how corporate events and their opinions influence equity volatility is significant. These comprise stock repurchases [102], primary equity offers [101], CEO turnover [104], quarterly earnings announcements [110], and internal control deficiencies [111]. However, little is documented about ISec's breaches on risks related to the firm's equity. Through understanding the connection between ISec breaches and equity volatility (risk), our research addresses the gap in the finance and information-system literature. Our third hypothesis is, therefore, the following:

Hypothesis 2 (H₂). *Firms with ISec breaches would face an elevated equity risk (σ_e^2).*

Figure 1 exhibits the conceptual framework of this study. The announcement of ISec breach as an exogenous construct. At the same time, long-run investors' confidence demonstrates the endogenous construct.

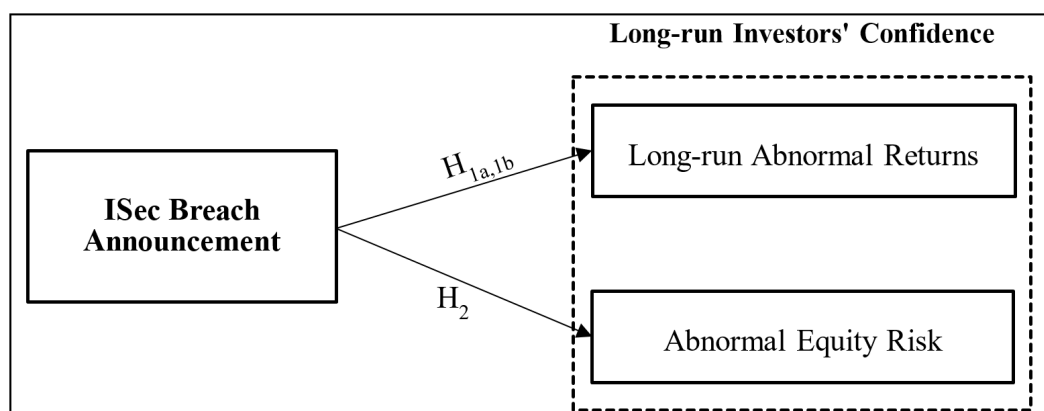


Figure 1. A conceptual framework for analyzing the impact of information security (ISec) breaches on long-run investors' confidence.

4. Methodology

In the case of ISec breach announcements, there could be a gradual adjustment in stock prices. Therefore, its exhaustive impact on the stock market and, thus, on the investors' confidence cannot be exhibited by the traditional event study methodology as examined by References [13,88]. The methods and estimation techniques we use in measuring the long-run abnormal returns are different from those usually used in event studies when the short-run impact of events is analyzed on the stock market. The event study methodology frequently provides skewed approximations of both the ultimate economic influence and the test statistics [97,98]. Our findings are based on robust and more accurate methods, which were newly established and used frequently in studies other than ISec [95,99,100,112–114].

4.1. Sample Selection

The sample data of firms suffering from ISec breaches were extracted from online data sources such as “The Privacy Rights Clearing House, Identity Theft Resource Centre, and Carnage”. The quest was carried out between 2011 and 2019 and scanned for announcements that encompass ISec breaches affecting the confidentiality, integrity, and availability of information systems. All ISec breach announcements by a firm should qualify the following in order to remain in our sample:

1. The firm is publicly listed in any of the stock exchange in US (i.e., New York Stock Exchange (NYSE) or the National Association of Securities Dealers Automated Quotations (NASDAQ)).
2. The firms must have returned information on the Center for Research on Security Prices (CRSP) database.
3. The firm must trade on at least 80 percent of their trading days within one year before the ISec breach announcement.
4. The firm did not report any other ISec breach within 18 months of this date of notification.
5. When the breach occurred on an unlisted subsidiary firm, the parent company was tracked.
6. The firm must have a book value greater than zero.

Criterion 4 was implemented to prevent duplication of announcements in the same period. We analyze each ISec breach's impact on a period that starts six months before through twelve months after the ISec breach announcement date. Thus, including ISec breach announcements that happened within eighteen months of each other will result in overlapping periods. Similar results counted more than once on the cumulative averages, which could theoretically skew our results.

We gathered our sample data from the sources mentioned in the beginning of this sub-section. A sample of 155 ISec breach events was gathered during 2011–2019 (Table 2). Using the selection criteria discussed above, these samples were then screened for long-run analysis. Due to confounding events in the range of 2 years before and after the ISec breach event, 59 samples were screened out. Furthermore, 19 samples were screened out as they have an overall time frame of less than one year, limiting the feasibility of long-run analysis. Among that, 15 samples of breached events from 2019 were screened out, as sufficient data to conduct a one-year analysis were not available. Lastly, four samples were withdrawn, as they could not meet our inclusion criteria, as discussed in Section 3. An example is breached firms with book values less than zero. In this way, long-run investors' confidence was assessed on a sample of 73 breached firms.

Among the firms with the highest number of breaches, Citigroup Inc. has been attacked four times, with the days of the incident being 8 August 2011, 17 March 2013, 17 July 2013, and 25 July 2016. Apple Inc. has been targeted four times, with the days of the incident being 4 September 2012, 22 July 2013, 25 February 2014, and 1 September 2014. American Express Corporation has been targeted three times, with the days of the incident being 13 July 2012, 25 March 2014, and 1 April 2014. Sony Company has been targeted four times; the days of the incident were 26 April 2011, 2 June 2011, 24 August 2014, and 24 November 2014. Twitter, Inc. was attacked four times. The event days were 1

February 2013, 4 December 2013, 5 December 2014, and 13 June 2016. Moreover, JP Morgan, Automatic Data Processing Inc., Facebook, and Capital One were breached two times each. Those breaches were 12 February 2013, 27 August 2014, 15 June 2011, 4 December 2013, 28 September 2018, 20 March 2019, 5 November 2014, and 6 February 2017, respectively.

Table 2. Sample selection criteria.

Year	Sample Size	Confounding Effect	Book Value < 0	Event Period < 1 Year
2011	8	5	0	0
2012	10	6	0	0
2013	11	7	1	1
2014	12	6	0	0
2015	15	5	1	1
2016	20	7	0	0
2017	26	11	0	1
2018	28	10	1	1
2019	25	2	1	15
Total	155	59	4	19

4.2. Assessing the Long-Run Abnormal Returns

The fundamental issue in long-run stock market studies is forecasting abnormal returns for the concerned firms included in our sample. Abnormal returns are hypothesized. An abnormal return is the difference between a stock return and a comparable benchmark return equivalent to zero over the concerned era. The benchmark is employed in controlling variables to support stock returns. The notion is that whatever appears unknown after controlling for the identified variables is abnormal and linked to the event being addressed. Anything which remains unexplained is known to be abnormal and can be related to the event.

The literature argues about the way long-run irregular returns can be calculated [23,97]. The first problem is the relevant variables to be controlled for calculating abnormal long-run returns. Previous studies on long-run stock valuation have been primarily controlled for its systemic risk (or beta). According to current research, the size, market-to-book ratio, and previous performance are imperative predictors of stock returns [115–117]. Therefore, the present consensus appears that abnormal returns have to be determined after controlling size, market-to-book ratio, and previous performance [100].

The second question is to grasp the statistical significance of abnormal long-run returns. Studies by References [97,98] noted that the test statistics of many widely employed approaches are highly flawed, making it challenging to comprehend the real significance of abnormal returns reported. The measurement error's principal cause is the cross-sectional correlation that exists due to overlaid periods between sampled firms, which typically occurs in long-run stock price examinations. Cross-sectional correlation leads to bias test statistics (positive or negative). Recent regression findings indicate that abnormal returns by one-to-one match sampling methodology [97,99] provide well-defined tests.

4.2.1. Buy-and-Hold Abnormal Returns (BHARs) Using One-to-One Match Samples

Our approach was one-to-one matching in which each sample firm is compared to the appropriate control firm having similar size, market-to-book ratio, and prior performance. Then we created two individual samples of one-to-one:

1. Choose a firm nearest in size to the sample firm from the sample firm's industry (size-matched).
2. Choose a firm nearest to the sample firm regarding its previous performance from the sample firm's industry (market-book ratio).

This paper provides an estimate of BHARs by daily return statistics as advocated by References [97,99]. BHAR calculation, therefore, requires that the sample firm's and its

matched control firm's raw returns be initially compounded over time. Mathematically, we get the following:

$$BHAR_i = \prod_{t=1}^T (1 + R_{it}) - \prod_{t=1}^T (1 + R_{mct}) \quad (1)$$

where $BHAR_i$ is the buy-and-hold abnormal return for stock i , R_{it} is the rate of return for stock i on day t , R_{mct} is the rate of return for the matched control firm for stock on day t , and T is the number of days in the period of interest. By summing the abnormal returns of all event samples, divided by the number of event samples (N), the average Buy-and-Hold Abnormal Returns are calculated by using the following expression.

$$\overline{BHAR}_{it} = \frac{1}{N} \sum_{i=1}^N BHAR_i \quad (2)$$

With the updated version of the standard t -test, the statistical value was assessed for results obtained by using the $BHAR$ process. The measurement formula developed by Reference [118] was employed here:

$$t = \frac{\overline{BHAR}_{it}}{\sqrt{\frac{\sigma_i^2}{N} + \frac{\sigma_{mc}^2}{N}}} \quad (3)$$

where σ_i^2 is the variance of firm i , and σ_{mc}^2 is the variance of the matched control firm.

4.3. Assessing the Equity Risk

The general approach in assessing the equity risk from the market perspective is by analyzing the volatility of equity stock returns concerning a corporate event. To determine any significant changes in equity risk, studies have analyzed the equity volatilities before and after the event [104,111]. Most researchers measure irregular deviation shifts by utilizing matched control samples to test the equity market and industrial factors.

The expectation that changes in volatility will occur after the report of the ISec violations is justifiable. Moreover, there might probably be some information leakage about ISec breaches prevalent in the market. Besides, the information risk, financial leverage, and operating levers might be effected in the light of ISec breaches. The volatility changes can be compared in the six months before (days -135 to -11) and after the ISec breach announcement (days $+11$ to $+260$). Furthermore, the volatility of six months before the announcement (days -135 to -10) should be compared with the volatility within one year (days $+10$ to $+260$) after the ISec breach announcement to analyze any significant deviations. The pre-announcement duration (i.e., days -135 to -11) is the period used as a base to evaluate volatility changes. The volatility changes are examined in the post-announcement period to assess if the shift in volatility is transient or irreversible. Volatility in each time-frame is the standard deviation of the regular returns of the firm's portfolio over that time. To predict standard deviations, a minimum of 125 daily returns should be accessible in one year. Standard deviation is a financial, statistical measurement that indicates the historical volatility of that investment compared to the average return.

$$\text{Standard Deviation (SD)} = \sqrt{\frac{\sum_{i=1}^n (x_i - \bar{x})^2}{n - 1}} \quad (4)$$

where x_i = return on an i th day for a firm's stock, \bar{x} = the average return in each period, and n = the number of days in the timeline.

Most of those papers which examine the impact of corporate events on changes in risk analyze the risk level of sampled firms comparing before and after the announcement date [102,103,119,120]. This strategy may misjudge actual risk adjustments, as certain macro-factor variables may not have anything to do with the event being considered. It

might comprise interest rates, investor views, consumer trust, industry, and business world perceptions. It is vital to compare the percentage changes in our sample firms' equity standard deviations to that of the matched control sample to handle these factors. To that end, the same two control samples used to measure the Buy-and-Hold Abnormal Returns by a one-to-one matching approach are used to estimate the changes in equity risk (see Section 4.2.1). These controls match size, matching performance, and matching samples for the industry (Figure 2). For each sample firm, we compare percentage changes in volatility as follows:

$$\% \Delta \text{ volatility} = \% \Delta \text{ in volatility of sample firm} - \% \Delta \text{ in volatility of control firm} \quad (5)$$

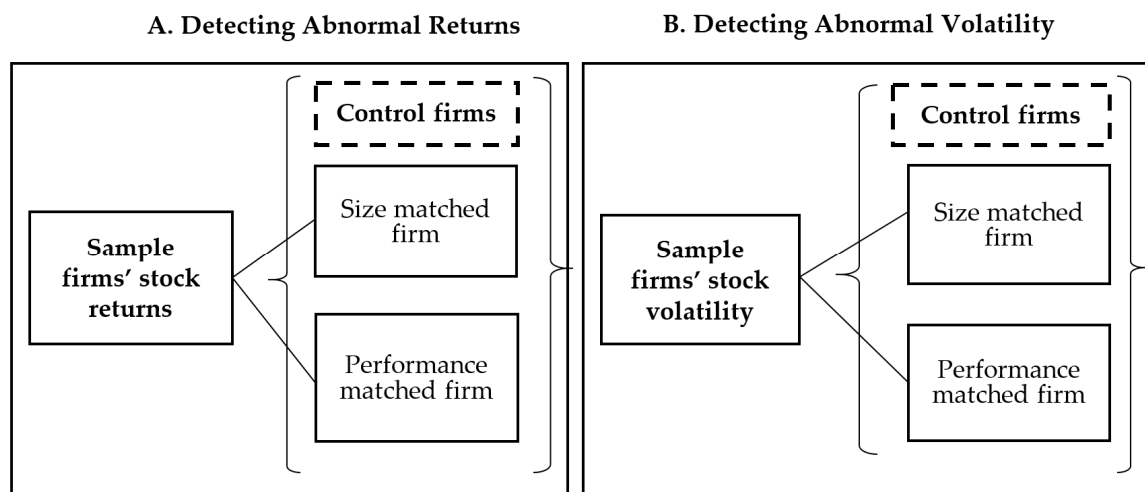


Figure 2. One-to-one matched sampling methodology [97].

4.4. Mapping of ISec-Events for Assessment of Investors' Confidence

To collect findings over time, we map the calendar to date for each entity's occurrence in our sample. The day of the announcement is day 0, the next day for trade is day 1, and the day before the announcement is day -1, and so on. It is advised to forecast abnormal returns and equity standard deviations for at least 18 months, beginning six months prior to announcements, through two periods of six months each after the ISec breach notification. It consists of 250 trading days each year.

Furthermore, it is contemplated to deduct from both sides a 2-week duration (10 trading days) while measuring abnormal changes in stock returns and equity volatility. It is advised to ensure that our assessments of investors' confidence cannot be unduly influenced by the unexpected trading practices that may occur around the announcement date. That is expected to give a more exact picture of investors' confidence in the long-run. It is fair to expect that there will be immediate changes in investors' confidence ensuing to notification of ISec breaches. It is also conceivable that the market will prevail over whether ISec breach announcements are likely to occur for a firm.

Moreover, ISec breaches may, in the period before the disclosure, have already impacted stock prices, and thus, the investors' confidence. Therefore, before the actual announcement, abnormal changes may occur (Figure 3). In the following three periods of six months each, we degree Buy-and-Hold Abnormal Returns and standard deviation from daily stock returns:

- Six months pre-announcement: trading days -135 to -11,
- Six months post-announcement: trading days 11 to 135,
- Twelve months post-announcement: trading days 136 to 260.

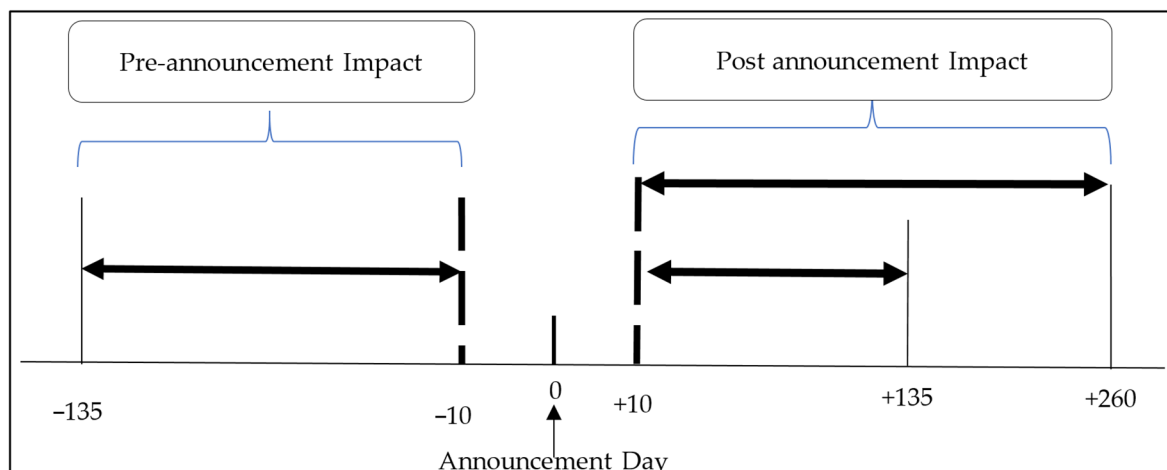


Figure 3. Mapping of calendar time for assessment of investors' confidence.

5. Results

The current paper has analyzed the long-run impact on the confidence of investors ensuing to ISec breaches that occurred from 2011 to 2019. Abnormal returns and equity risk demonstrates the investors' long-run confidence. This study's principal objective was to explore whether the announcement of ISec breaches influences the long-run confidence of investors.

Table 3 presents statistics on the sample based on the most recent fiscal year completed before the date of the ISec breach announcement. The mean (median) observation represents a firm with annual sales of nearly \$52,495 million (\$21,285.6 million), total assets of \$501,915.3 million (\$60,850 million), and net income of \$6127 million (\$2887 million).

Table 3. Summary statistics of the sample.

Measure	Mean	Median	Standard Deviation	Minimum	Maximum
Sales (\$million)	52,495.0	21,285.6	62,370.5	96.3	2,997,148
Equity market value (\$million)	85,7688.8	32,019.2	105,775.9	108.5	823,027.9
Total assets (\$million)	501,915.3	60,850	590,815	101.5	2,998,788
Operating income (\$million)	6127	2887	6227.3	−1579	45,781
Market to Book	6.1	2.1	19.5	0.8	150.6

This section depicts the results of abnormal returns and abnormal equity standard deviations for our sample firms matched with their respective control firms. Using a one-to-one matching approach, stock returns and standard deviations were matched to an appropriately chosen control firm.

5.1. Evidence of Long-Run Abnormal Returns

As mentioned previously, each sample firm has two different control samples to fit a controller based on proximity in sizes and performance from the same industry. The results can be found in Table 4. Since the findings in the two controls are quite similar, we have

focused our discussion on the size-matched control sample in our argument. When sample firms are matched on size, the mean abnormal returns in the period before the ISec breach are 4% positive, but they were not significant. At the same time, 40% of the sample firms experience negative abnormal performance. Therefore, H_{1a} is rejected. It means that there will have no effect on stock returns before ISec breach announcement. However, in the period after the announcement, i.e., within six months of the announcement, sample firms have negative abnormal returns, with nearly 60% of sample firms having negative abnormal returns. The mean abnormal returns were negative at 15%. These performance levels were significant at 5% level (t-statistic = -3.81). Likewise, significant negative abnormal returns of 18.5% (t-statistic = -4.98) were found in the next six months (i.e., 136 days to 260 days), with 55% of the sample firms experience significant negative abnormal returns. Hence H_{1b} is accepted. In general, the average abnormal return over eighteen months was -12.5% (t-statistic = -2.97), and nearly 57% of sample companies had negative abnormal returns.

Table 4. Long-run abnormal returns of sample firms matched with control firms.

	Size-Matched Control Firm				Performance-Matched Control Firm			
	Observations	Mean	%Negative	t	Observations	Mean	%Negative	t
Six months before announcement (days -136 to -11)	73	0.04	40%	1.45	73	-0.136	52%	-1.37
Six months after announcement (days 11 to 135)	73	-0.15	60%	-3.81	73	-0.063	58%	-4.23
Twelve months after announcement (days 136 to 260)	73	-0.185	55%	-4.98	73	-0.125	60%	-2.96
Six months before through twelve months after the announcement (days -136 to 260)	73	-0.125	57%	-2.97	73	-0.09	55%	-1.99

The findings are consistent with earlier research [121,122]. The results showed that investors' short-run response did not adequately exhibit the announcement effect and was balanced over the long run. The findings are consistent with earlier research [100,113,121,122]. In the context of information security, results are similar to those concluded by Reference [92]. It can be inferred that investors underestimated the detrimental impact of an ISec breach initially. According to [123], inefficiencies in a market result from arbitrage limitations and information processing bias by investors [124]. Reference [98] also claimed that "continuous behavioral biases can take a long time, and arbitration forces can rectify the mispricing". The findings of this study affirm H_{1b} that the announcement of a breach has a substantial negative impact on the long-run confidence of investors of breached firms. If investors buy and hold the firm's stock after the incident: In six months, they will suffer a -15% loss; holding twelve months will expand the loss to -18.5% , respectively.

5.2. Evidence of Changes in Equity Standard Deviations

To evaluate equity risk on sample firms after an ISec breach announcement, we analyzed the volatility changes in sample firms to a matched control sample firm. Table 5 depicts such statistics using two separate control samples as benchmarking. Abnormal volatility change is then the difference between the percent change in the equity standard deviation of the sample firm and its matched control firm. Abnormal equity standard deviations are depicted in two intervals here. One is the six months before and after the ISec breach announcement.

Table 5. Abnormal standard deviation of sample firms matched with control firms.

Performance Statistics of Changes in Equity Standard Deviation (σ_e)	Time Period	
	Six Months before through Six Months after the ISec Breach Announcement	Six Months before through Twelve Months after the ISec Breach Announcement
Relative to the size-matched control sample		
Number of observations	73	73
Mean abnormal change in standard deviation	0.135	0.07
% of abnormal changes that are positive	58%	40%
t-statistic	7.54	1.47
Relative to the performance-matched control sample		
Number of observations	73	73
Mean abnormal change in standard deviation	0.109	0.0673
% of abnormal changes that are positive	52%	44%
t-statistic	6.38	0.6351

In comparison, other period analyzes the abnormal equity standard deviations that starts six months before the ISec breach announcement to 12 months after the announcement. The estimation of data was based on parametrical as well as non-parametric testing. Likewise, the results for abnormal returns, the outcomes for equity deviations in the two control samples are quite similar; the results of the size-matched control sample are the subject of our discussion.

During the six-monthly pre- and post-announcement period, the average change in equity standard deviations of sample firms compared to control firms was positive. The mean abnormal change in equity standard deviation is 13.5%, significant at 5% (t-statistic = 7.54). In comparison, the median shift in the equity standard deviation is 9.8%, significant at 5% (the Z-statistical figure for the Wilcoxon signed-rank test is 6.93). The abnormal shifts are 58.82% positive and substantially different from 50% at 5% (Z-statistic of the Binomial sign test is 5.03). Accordingly, the parametric and non-parametric measures suggest a substantial rise in equity risk for six months before and after the ISec breach announcement. The higher risk over this duration may have contributed in part to the negative abnormal returns we see over this duration.

When we look at the equity changes for six months before the announcement to twelve months after the announcement, the outcomes are much different. Despite observing positive changes in mean and median during this period, none of those changes were significant at the conventional five percent level (t-statistic = 1.47). For a variety of reasons, this is an exciting outcome. First, it suggests that a considerable rise in equity risk is witnessed when the ISec breaches are officially reported. Second, the spike in standard equity deviations between the six months before and after the announcement is not attributed to a non-stationary range of standard deviations. There were statistically no noticeable differences in standard deviations between six months before and 12 months after the announcement. Finally, there is no temporary rise in equity risk in six months before and after the announcement, since the risk is not decreased in the following months. Firms were encountering a lower level of equity risk before ISec breaches, however. ISec breaches raise the business risk and, thus, the following months' equity risk. Therefore,

H₂ is accepted to the extent that the equity risk will stand at a higher level for at least six months after an ISec breach.

6. Discussion of Findings

This study sought to answer the research question that concerns the long-run impact of ISec breach announcements on the confidence of investors. The study is, therefore, aimed at achieving two research objectives. The first objective aims to evaluate the long-run impact of ISec breach on long-run abnormal returns of breached firms. Grounded on a sample of 73 ISec breaches reported by publicly traded firms during 2011–2019, we examine its long-run impact on investors' confidence exhibited by stock returns over eighteen months, starting six months before the announcement through twelve months after the announcement. Using one-to-one matched sampling methodology, the findings indicated that the breached firm, as compared to its matched control firm, will suffer negative abnormal returns ranging between -15 and -18.5% over a one-year post-announcement period. However, there was no significant evidence as to any abnormal stock returns in the pre-announcement period. The second research objective aims to evaluate the long-run impact of the ISec breach on the breached firm's equity risk. Using abnormal stock returns volatility as a proxy for equity risk, the findings indicated that the breached firm, as compared to its matched control firm, will be confronted with an 11% higher equity risk over six months before and after the announcement. This section puts forward the theoretical and practical implications of these findings in Sections 6.1 and 6.2, respectively. Lastly, Section 6.3 discusses the study limitations and directions for future research.

6.1. Theoretical Contribution

This paper looks at the ISec breaches' impact on investors' confidence, as shown by long-run abnormal returns on stock and equity risk. In the area of ISec, several studies have examined the effect of breach events on investors' short-run confidence based on short-run abnormal returns. Whereas few [92] have investigated investors' long-run confidence in such events. Nevertheless, the current study has used a one-to-one matched sampling methodology, which is more robust in analyzing the confidence of investors in the long run. According to this method, results (in our case, long-run abnormal returns and equity standard deviations) of each sample firm is matched with a respective control firm before drawing any noteworthy conclusion. It was revealed that the breached firms would suffer unfavorable consequences, in the form of negative abnormal returns (-18%) and higher equity risk (11%), in the one year after an announcement. In this way, the study is an extension of EMH theory, by advocating that unexpected events can have a long-run impact on the stock market. Therefore, stock prices do incorporate the effect of information not only in the short run but also in the long run.

Our findings exhibited that the long-run abnormal returns will be negative over one year after an announcement. This finding is, to some extent, similar to those concluded by Reference [92], using event study methodology. However, for a few reasons, we believe that the long-run abnormal returns, as observed in the current study, are more compelling and reliable. First, a more robust methodology of one-to-one-matched sampling is employed for long-run analysis. The former computed the abnormal returns through event study methodology in which the sample firms' returns were matched with a benchmark of a market index. There is an influential research group that advocates that size and market-to-book ratio [116] and prior performance [115,117] are major estimators of stock returns. Thus, the sample firms' returns should be matched with similar firms having similar size and performance. Our study has followed the same consensus that abnormal returns should be estimated after controlling for size, market-to-book ratio, and prior performance [99]. Second, the statistical significance of the long-run abnormal returns observed is difficult to interpret. References [97,98] report on the severely misspecified testing statistics from many widely used methods, making it difficult to assess the true significance of observed abnormal returns. The existence of cross-sectional dependence

resulting from the overlap between sampling firms seen in long-term stock price studies is a primary cause of misspecification. Cross-sectional (positive or negative) dependence contributes to testing statistics that are skewed. The literature's simulation results indicate that abnormal returns determined using one-to-one matching provide well-specified tests [97,99]. For these reasons, we can claim that the study findings are robust and more accurate than previous research.

This study also examines ISec breaches' impact on firm risk by analyzing the adjustments in equity volatility associated with ISec breaches. Most of the previous studies concentrated on stock price performance and operational performance, ensuing to ISec breaches. This study examines the foremost consequences of ISec breaches on equity risk (volatility). The higher equity risk, as depicted from this study elaborates in part to the negative abnormal returns we see over the six-monthly period after an announcement. Given that stock fluctuations may have substantial effects on the firm and its stakeholder, it is essential to recognize these consequences in designing and implementing overall information systems. Reducing the extent or magnitude of ISec breaches will limit the firm's exposure to the negative impacts of increased volatility. This includes investment in improving new technologies, such as awareness of ISec and the capacity to detect and respond more effectively to ISec breaches. A further theoretical implication of the above findings is that the increased volatility associated with ISec breaches may raise capital costs.

Given that the whole rise in abnormal volatility is expressed in the cost of capital, sample firms' capital expense will rise by 11% compared to the controls. Conversely, this will decrease the equity value of sample firms by 11%. Taking SONY as an example, this reveals that SONY's loss of market value of 293 million dollars a year after the incident and total loss of 937 million two years after the event would result from an ISec breach event. This study's findings indicate that ISec violation incidents have significant adverse effects on the long-run confidence of investors and the long-run valuation of the company. Investors would reevaluate the company's worth in the stock exchange as they face tangible and intangible risks from ISec's breach incidents. This analysis should then be a benchmark assuming that management will consider the quality of investment in ISec in the firm's market valuation more carefully.

6.2. Practical Contribution

Our examination of the long-run confidence of investors is practically significant for a few reasons. The estimates based on long skylines are more of value to investors and managers. It furnishes them with a progressively wide-ranging image of the financial ramifications of ISec breaches. By investigating the long-run impact of ISec breaches, we have revealed some insight into the timeline of abnormal stock price performance as far as when it begins, to what extent it keeps going, and whether firms recuperate ISec breaches rapidly. Our results revealed that the event of ISec breach would affect the confidence of investors in the post-announcement period (i.e., from six months to one year). Nevertheless, we do not find any significant abnormality in the confidence of investors in the pre-announcement period. These findings are significant in setting practical anticipations concerning the possible ramifications of ISec breaches.

Second, these findings emphasize the significance of ISec and determine that it cannot be disregarded. Events of ISec breach do not occur unwittingly, and over time, users have a lower level of tolerance for such events. Moreover, the news or media attention exposes the presence of flaws in the firm's ISec, rendering the firm more likely to be the victim of such assaults in the future. ISec breaches are expected to continue and grow further along with the invention of breach techniques. Breached firms are also confronted with legal action risks, charges of litigation, reconstruction, and other expenditures. These all influence investor confidence in the long run, and hence on the stock valuation of the company. For instance, there is a record size of 70 million data files revealed in recent events such as Target's data breach in 2013, with a legal settlement of about \$39 million [125]. Likewise, in 2014, Home Depot's data of 56 million elements were breached, resulting in a legal

payout of \$13 million [126]. Likewise, the case with Equifax is discussed in Section 1.1. From these three large-scale breaches, we can conclude that the effect lasted for at least a year following ISec breaches' disclosure before litigation of the punitive damages for the follow-up. As per the authors' best knowledge, the current study is the pioneer study to explore such a long-run effect. We believe that this study's findings will allow firms to effectively determine the right level of ISec investment to safeguard sensitive data and personal information about their customers.

Lastly, our findings also revealed a higher level of equity risk for breached firms than its matched control firm. The rise in equity volatility resulting from ISec breaches might lead to an increase in the financial and operational leverage of the firm. Accordingly, firms can take counterbalancing measures to reduce financial leverage by issuing additional equity or retiring the debt. Likewise, augmented operating leverage can be neutralized by adjusting the firm's cost structure (lessen fixed or variable costs). Changes in financial and operational indicators can be costly, and the future advantages of reduced stock volatility should be weighed against these costs.

6.3. Limitations of the Study and Future Research Directions

In this study, there are certain limitations and future research needs. Despite analyzing sample firms' performance through a one-to-one matching approach, there could still be an endogeneity problem. The matching portfolio approach can further improve future research reliability for forecasting investors' confidence ensuing to an ISec breach.

Second, our sample comes from breached firms listed in US stock exchanges such as NASDAQ, NYSE, and AMEX. The impact of our findings can, therefore, not be applied to other countries' stock exchanges at this point. Furthermore, the most frequent occurrence was in 2014 concerning the sample distribution gathered in this study. Such distribution reduces the number of samples to approximate the different long-run valuation intervals and results in a minimal long-run survey.

Future research can also explore the influence on long-run investors' confidence concerning contingency factors of ISec breach. For example, future studies can examine the impact on investors' confidence in the light of ISec breach contingency factors such as type of breach, firm characteristics, and type of industry. Past studies have found a significant impact of these factors on short-run investors' confidence. It will be interesting to explore how the abnormality in investors' confidence is influenced in the long-run by ISec contingency factors. Future studies can also analyze in detail the long-run impact on investors' confidence ensuing to other types of breach events such as phishing, Advanced Persistent Threat (APT), computer viruses, and DoS attacks. Researchers who are interested in exploring this issue are urged to follow this thread.

Moreover, an extensive research avenue still exists concerning the financial impact of ISec regulations or frameworks being announced by regulators. An attempt has been made by Reference [127] by examining the short-run influence on the firm value ensuing to ISec legislations in the healthcare sector. Likewise, researchers can examine the long-run financial impact of such legislation in other vulnerable sectors such as Internet-based firms and the firms in the financial and energy sector. Perhaps, imposed ISec legislations at one end can provide some long-run assurance of ISec but, on another end, will require hefty investments by firms on account of the system upgrade, employee training and so on. Therefore, it will be exciting to delve into the behavior of investors ensuing in such regulations.

Future studies in this area could be an integration of security breach and security investment event; how the security investment events play their role in mitigating the loss in investors' confidence ensuing to an ISec breach. Likewise, cyber-insurance is an emerging phenomenon. Future research can contemplate the role of cyber insurance as a moderating factor in mitigating the stock losses at the event of a security breach. Likewise, the impacts of ISec-events should be investigated on the firm performance concerning profitability and activity. In general, we have concluded that even though the influence of

ISec-events on the stock market is critical, severe, and stimulating, the studies related to it are less in numbers. Therefore, the field is vast and open to applying more sophisticated, innovative, and compelling research methodologies.

7. Conclusions

This paper addresses the challenges of ISec confronted by firms, which could hurt sustainable economic growth. ISec is a substantial distinguishing factor for firms and is a critical sustainable economic development factor, according to the literature. This article addresses the challenges of information security, especially for publicly traded companies, which could affect sustainable economic growth. Using a sample of 73 ISec breach announcements, the current study examines the long-run impact of ISec breach events on the confidence of investors, as expressed by an abnormality in long-run stock returns and equity risk. We find negative abnormal returns (−15 to −18%), following the twelve months after the announcements of the ISec breach. Furthermore, a rise in equity risk (10%) was also noted for sample firms, compared to their matched control firms in the six-monthly pre- and post-announcement.

The adverse economic effects of ISec breaches and the lack of proof of a successful turnaround reinforce the need to pay careful attention to the threat of ISec breaches. Today, information systems are conceivably more vulnerable to ISec breaches than they were previously. While serious ISec breaches are not common, they can seriously hinder a firm's stock performance and decrease investor confidence in the years ahead. Firms must do whatever they can to avoid significant intrusions of ISec and reduce the extent of the breach of ISec. Moreover, companies must establish the ability to anticipate ISec breaches, including the detection, classification, and oversight of any ISec compliance incidents affecting internal processes, vendors, and customers. Because the harmful effects of ISec breaches are exacerbated when breaches remain undetected, firms must develop the ability to learn earlier and better about ISec breaches and aspire for a time interval of zero between an ISec breach and its identification. Sooner or later, firms must cope with ISec breaches' challenges and strategies to prevent the worsening and degradation of the situation. For this, a systematic approach must be developed to deal with and respond to ISec breaches, with clear identification of liability and resource allocation and learnings from previous ISec breaches, the prediction of ISec breaches, and the prevention of adverse economic impacts of ISec breaches. Traditional approaches to ISec are based on reporting intrusions, i.e., "incident response", after the attack. Nevertheless, a more constructive approach is needed nowadays; in other words, preventive action needs to be put in place. ISec should be viewed as a matter of corporate social responsibility by firms to protect their customers, investors, and sustainable growth.

Author Contributions: Conceptualization, S.E.A.A. and F.-W.L.; methodology, S.E.A.A. and F.-W.L.; validation, F.-W.L. and M.K.S.; writing—original draft preparation, S.E.A.A.; writing—review and editing, S.E.A.A., R.H., and M.K.S.; visualization, R.H. and M.K.S.; supervision, F.-W.L. All authors have read and agreed to the published version of the manuscript.

Funding: This work was funded by the Department of Management and Humanities, Universiti Teknologi PETRONAS (UTP), and Faculty of Business and Economics, Universitas Islam Indonesia (UII), under grant cost center 015MEO-114. The APC was funded through this grant.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Publicly available data has been extracted from Privacy Rights Clearing House (PRCH) and were used to analyze the long-run impact of information security breaches. This data can be found at: <https://privacyrights.org/data-breaches>.

Acknowledgments: The authors would also like to thank the reviewers for their valuable suggestions to enhance the manuscript. We would also like to thank the Institute of Self-Sustainable Building (ISB), UTP and Centre of Social Innovation (COSI), UTP and Universiti Utara Malaysia (UUM) to facilitate this research study.

Conflicts of Interest: The authors declare no conflict of interest.

References

- Dalampira, E.S.; Nastis, S.A. Mapping sustainable development goals: A network analysis framework. *Sustain. Dev.* **2020**, *28*, 46–55. [CrossRef]
- Minges, M.; Korke, D.; Fondeur, S. UNCTAD Technical Notes on ICT for Development. Available online: https://unctad.org/system/files/officialdocument/tn_unctad_ict4d06_en.pdf (accessed on 1 April 2016).
- UN. *Transforming Our World: The 2030 Agenda for Sustainable Development*; United Nations General Assembly: New York, NY, USA, 2015.
- Shad, M.K.; Lai, F.-W.; Fatt, C.L.; Klemeš, J.J.; Bokhari, A. Integrating sustainability reporting into enterprise risk management and its relationship with business performance: A conceptual framework. *J. Clean. Prod.* **2019**, *208*, 415–425. [CrossRef]
- OECD/WTO. *Aid for Trade at a Glance 2017—Promoting Trade, Inclusiveness and Connectivity for Sustainable Development*; OECD Publishing: Paris, France, 2017.
- Evangelista, R.; Guerrieri, P.; Meliciani, V. The economic impact of digital technologies in Europe. *Econ. Innov. N. Tech.* **2014**, *23*, 802–824. [CrossRef]
- Demekas, D.G. Emerging Technology-Related Issues in Finance and the IMF—A Stocktaking. Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3330190 (accessed on 24 February 2019).
- Fama, E.F.; French, K.R. Dissecting anomalies. *J. Financ.* **2008**, *63*, 1653–1678. [CrossRef]
- Savoie, M. Security. In *Building Successful Information Systems: Five Best Practices to Ensure Organizational Effectiveness and Profitability*, 2nd ed.; Business Expert Press: New York, NY, USA, 2016. [CrossRef]
- Ponemon Institute. *Cost of a Data Breach Report*; IBM Security: North Traverse City, MI, USA, 2020.
- Cavusoglu, H.; Mishra, B.; Raghunathan, S. The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. *Int. J. Electron. Commer.* **2004**, *9*, 70–104. [CrossRef]
- Smith, K.T.; Jones, A.; Johnson, L.; Smith, L.M. Examination of cybercrime and its effects on corporate stock value. *J. Inf. Commun. Ethics Soc.* **2019**, *17*, 42–60. [CrossRef]
- Bose, I.; Leung, A.C.M. Do phishing alerts impact global corporations? A firm value analysis. *Decis. Support. Syst.* **2014**, *64*, 67–78. [CrossRef]
- Ettredge, M.; Richardson, V.J. Assessing the risk in e-commerce. In Proceedings of the Annual Hawaii International Conference on System Sciences, Big Island, HI, USA, 10 January 2002; pp. 1–11.
- Campbell, K.; Gordon, L.A.; Loeb, M.P.; Zhou, L. The economic cost of publicly announced information security breaches: Empirical evidence from the stock market. *J. Comput. Secur.* **2003**, *11*, 431–448. [CrossRef]
- Hovav, A.; D’Arcy, J. The impact of virus attack announcements on the market value of firms. *Inf. Syst. Secur.* **2004**, *13*, 32–40. [CrossRef]
- Kannan, K.; Rees, J.; Sridhar, S. Market reactions to information security breach announcements: An empirical analysis. *Int. J. Electron. Commer.* **2007**, *12*, 69–91. [CrossRef]
- Malhotra, A.; Kubowicz Malhotra, C. Evaluating customer information breaches as service failures: An event study approach. *J. Serv. Res.* **2011**, *14*, 44–59. [CrossRef]
- Sinanaj, G.; Muntermann, J. Assessing corporate reputational damage of data breaches: An empirical analysis. In Proceedings of the 26th Bled EConference—EInnovations Challenges and Impacts for Individuals, Organizations and Society, Bled, Slovenia, 9–13 June 2013; pp. 78–89.
- Tweneboah-Kodua, S.; Atsu, F.; Buchanan, W. Impact of cyberattacks on stock performance: A comparative study. *Inf. Comput. Secur.* **2018**, *26*, 637–652. [CrossRef]
- Fama, E.F.; Fisher, L.; Jensen, M.C.; Roll, R. The adjustment of stock prices to new information. *Int. Econ. Rev.* **1969**, *10*, 1–21. [CrossRef]
- Schwartz, R.A. Efficient capital markets: A review of theory and empirical work: Discussion. *J. Financ.* **1970**, *25*, 421–423. [CrossRef]
- Fama, E.F. Market efficiency, long-term returns, and behavioral finance. *J. Finan. Econ.* **1998**, *49*, 283–306. [CrossRef]
- Robert, A.; Haugen, N.L.B. Case closed. In *Handbook of Portfolio Construction: Contemporary Applications of Markowitz Techniques*; Springer Science & Business Media: Anchorage, AK, USA, 2009.
- Shiller, R.J. Measuring bubble expectations and investor confidence. *J. Psych. Fin. Mark.* **2000**, *1*, 49–60. [CrossRef]
- Hendricks, K.B.; Singhal, V.R. The effect of supply chain glitches on shareholder wealth. *J. Oper. Manag.* **2003**, *21*, 501–522. [CrossRef]
- Galai, D.; Masulis, R.W. The option pricing model and the risk factor of stock. *J. Finan. Econ.* **1976**, *3*, 53–81. [CrossRef]
- Smith, C.W., Jr.; Warner, J.B. On financial contracting: An analysis of bond covenants. *J. Finan. Econ.* **1979**, *7*, 117–161. [CrossRef]
- Gordon, L.A.; Loeb, M.P. Budgeting process for information security expenditures. *Commun. ACM* **2006**, *49*, 121–125. [CrossRef]

30. Gordon, L.A.; Loeb, M.P. The economics of information security investment. *ACM Trans. Inf. Syst. Secur.* **2002**, *5*, 438–457. [[CrossRef](#)]
31. Hsu, C.; Lee, J.N.; Straub, D.W. Institutional influences on information systems security innovations. *Inf. Syst. Res.* **2012**, *23*, 918–939. [[CrossRef](#)]
32. Wang, T.; Kannan, K.N.; Ulmer, J.R. The association between the disclosure and the realization of information security risk factors. *Inf. Syst. Res.* **2013**, *24*, 201–218. [[CrossRef](#)]
33. Gordon, L.A.; Loeb, M.P.; Sohail, T. Market value of voluntary disclosures concerning information security. *MIS Q.* **2010**, *34*, 567–594. [[CrossRef](#)]
34. Lowry, P.B.; Cao, J.; Everard, A. Privacy concerns versus desire for interpersonal awareness in driving the use of self-disclosure technologies: The case of instant messaging in two cultures. *J. Manag. Inf. Syst.* **2011**, *27*, 163–200. [[CrossRef](#)]
35. Hovav, A.; D’Arcy, J. Capital market reaction to defective IT products: The case of computer viruses. *Comput. Secur.* **2005**, *24*, 409–424. [[CrossRef](#)]
36. Deane, J.K.; Goldberg, D.M.; Rakes, T.R.; Rees, L.P. The effect of information security certification announcements on the market value of the firm. *Inf. Technol. Manag.* **2019**, *20*, 107–121. [[CrossRef](#)]
37. Goldstein, J.; Chernobai, A.; Benaroch, M. An event study analysis of the economic impact of IT operational risk and its subcategories. *J. Assoc. Inf. Syst.* **2011**, *12*, 606–631. [[CrossRef](#)]
38. Cao, J.; Calderon, T.; Chandra, A.; Wang, L. Analyzing late SEC filings for differential impacts of IS and accounting issues. *Int. J. Account. Inf. Syst.* **2010**, *11*, 189–207. [[CrossRef](#)]
39. Chai, S.; Kim, M.; Rao, H.R. Firms’ information security investment decisions: Stock market evidence of investors’ behavior. *Decis. Support. Syst.* **2011**, *50*, 651–661. [[CrossRef](#)]
40. Goel, S.; Shawky, H.A. Estimating the market impact of security breach announcements on firm values. *Inf. Manag.* **2009**, *46*, 404–410. [[CrossRef](#)]
41. Hovav, A.; Gray, P. The ripple effect of an information security breach event: A stakeholder analysis. *Commun. Assoc. Inf. Syst.* **2014**, *34*, 893–912. [[CrossRef](#)]
42. Hovav, A.; Andoh-Baidoo, F.K.; Dhillon, G. Classification of security breaches and their impact on the market value of firms. In Proceedings of the 6th Annual Security Conference, Las Vegas, NV, USA, 11–12 April 2007.
43. Telang, R.; Wattal, S. An empirical analysis of the impact of software vulnerability announcements on firm stock price. *IEEE Trans. Softw. Eng.* **2007**, *33*, 544–557. [[CrossRef](#)]
44. Hovav, A.; D’Arcy, J. The impact of denial-of-service attack announcements on the market value of firms. *Risk Manag. Insur. Rev.* **2003**, *6*, 97–121. [[CrossRef](#)]
45. Garg, A.; Curtis, J.; Halper, H. Quantifying the financial impact of IT security breaches. *Inf. Manag. Comput. Secur.* **2003**, *11*, 74–83. [[CrossRef](#)]
46. Acquisti, A.; Friedman, A.; Telang, R.J.I.P. Is there a cost to privacy breaches? An event study. In Proceedings of the 27th International Conference on Information Systems, Milwaukee, WI, USA, 10–13 December 2006.
47. Tanimura, J.K.; Wehrly, E.W. The market value and reputational effects from lost confidential information. *Int. J. Financ. Manag.* **2009**, *5*, 18–35. [[CrossRef](#)]
48. Hinz, O.; Nofer, M.; Schiereck, D.; Trillig, J. The influence of data theft on the share prices and systematic risk of consumer electronics companies. *Inf. Manag.* **2015**, *52*, 337–347. [[CrossRef](#)]
49. Yayla, A.A.; Hu, Q. The impact of information security events on the stock value of firms: The effect of contingency factors. *J. Inf. Technol.* **2011**, *26*, 60–77. [[CrossRef](#)]
50. Lin, Z.; Sapp, T.R.; Ulmer, J.R.; Parsa, R. Insider trading ahead of cyber breach announcements. *J. Financ. Mark.* **2019**, *50*, 100527–100541. [[CrossRef](#)]
51. Agrawal, A.; Jaffe, J.F.; Mandelker, G.N. The post-merger performance of acquiring firms: A re-examination of an anomaly. *J. Financ.* **1992**, *47*, 1605–1621. [[CrossRef](#)]
52. Draper, P.; Paudyal, K. Acquisitions: Private versus public. *Eur. Financ. Manag.* **2006**, *12*, 57–80. [[CrossRef](#)]
53. Lehn, K.M.; Zhao, M. CEO turnover after acquisitions: Are bad bidders fired? *J. Financ.* **2006**, *61*, 1759–1811. [[CrossRef](#)]
54. Loughran, T.; Vijh, A.M. Do long-term shareholders benefit from corporate acquisitions? *J. Financ.* **1997**, *52*, 1765–1790. [[CrossRef](#)]
55. Boehme, R.D.; Sorescu, S.M. The long-run performance following dividend initiations and resumptions: Underreaction or product of chance? *J. Financ.* **2002**, *57*, 871–900. [[CrossRef](#)]
56. Ikenberry, D.; Lakonishok, J.; Vermaelen, T. Market underreaction to open market share repurchases. *J. Financ. Econ.* **1995**, *39*, 181–208. [[CrossRef](#)]
57. Ikenberry, D.L.; Ramnath, S. Underreaction to self-selected news events: The case of stock splits. *Rev. Financ. Stud.* **2002**, *15*, 489–526. [[CrossRef](#)]
58. Kryzanowski, L.; Zhang, H. Market behaviour around Canadian stock-split ex-dates. *J. Empir. Financ.* **1993**, *1*, 57–81. [[CrossRef](#)]
59. Michaely, R.; Thaler, R.H.; Womack, K.L. Price reactions to dividend initiations and omissions: Overreaction or drift? *J. Financ.* **1995**, *50*, 573–608. [[CrossRef](#)]
60. Bradley, D.J.; Jordan, B.D.; Yi, H.C.; Roten, I.C. Venture capital and IPO lockup expiration: An empirical analysis. *J. Financ. Res.* **2001**, *24*, 465–493. [[CrossRef](#)]
61. Dharan, B.G.; Ikenberry, D.L. The long-run negative drift of post-listing stock returns. *J. Financ.* **1995**, *50*, 1547–1574. [[CrossRef](#)]
62. Ritter, J.R. The long-run performance of initial public offerings. *J. Financ.* **1991**, *46*, 3–27. [[CrossRef](#)]

63. Teoh, S.H.; Welch, I.; Wong, T.J. Earnings management and the long-run market performance of initial public offerings. *J. Financ.* **1998**, *53*, 1935–1974. [[CrossRef](#)]
64. Espenlaub, S.; Gregory, A.; Tonks, I. Re-assessing the long-term underperformance of UK Initial Public Offerings. *Eur. Financ. Manag.* **2000**, *6*, 319–342. [[CrossRef](#)]
65. Muntermann, J.; Roßnagel, H. On the effectiveness of privacy breach disclosure legislation in Europe: Empirical evidence from the US stock market. In Proceedings of the Nordic Conference on Secure IT Systems, Oslo, Norway, 14–16 October 2009; pp. 1–14.
66. Liginlal, D.; Sim, I.; Khansa, L. How significant is human error as a cause of privacy breaches? An empirical study and a framework for error management. *Comput. Secur.* **2009**, *28*, 215–228. [[CrossRef](#)]
67. Gatzlaff, K.M.; McCullough, K.A. The effect of data breaches on shareholder wealth. *Risk Manag. Insur. Rev.* **2010**, *13*, 61–83. [[CrossRef](#)]
68. Patel, N. The effect of IT hack announcements on the market value of publicly traded corporations. *Duke J. Econ. April* **2010**, *22*, 1–25.
69. Bolster, P.; Pantalone, C.H.; Trahan, E.A. Security breaches and firm value. *J. Bus. Valuat. Econ. Loss Anal.* **2010**, *5*, 1–13. [[CrossRef](#)]
70. Andoh-Baidoo, F.K.; Amoako-Gyampah, K.; Osei-Bryson, K.M. How internet security breaches harm market value? *IEEE Secur. Priv.* **2010**, *8*, 36–42. [[CrossRef](#)]
71. Smith, K.T.; Smith, L.M.; Smith, J.L. Case studies of cybercrime and their impact on marketing activity and shareholder value. *Acad. Mark. Stud. J.* **2011**, *15*, 67–82.
72. Morse, E.A.; Raval, V.; Wingender, J.R. Market price effects of data security breaches: A global perspective. *Inf. Secur. J.* **2011**, *20*, 263–273. [[CrossRef](#)]
73. Gordon, L.A.; Loeb, M.P.; Zhou, L. The impact of information security breaches: Has there been a downward shift in costs? *J. Comput. Secur.* **2011**, *19*, 33–56. [[CrossRef](#)]
74. Wang, T.; Ulmer, J.R.; Kannan, K. The textual contents of media reports of information security breaches and profitable short-term investment opportunities. *J. Organ. Comput. Electron. Commer.* **2013**, *23*, 200–223. [[CrossRef](#)]
75. Goel, S.; Shawky, H.A. The impact of federal and state notification laws on security breach announcements. *Commun. Assoc. Inf. Syst.* **2014**, *34*, 37–50. [[CrossRef](#)]
76. Pirounias, S.; Mermigas, D.; Patsakis, C. The relation between information security events and firm market value, empirical evidence on recent disclosures: An extension of the GLZ study. *J. Inf. Secur. Appl.* **2014**, *19*, 257–271. [[CrossRef](#)]
77. Arcuri, M.C.; Brogi, M.; Gandolfi, G. The effect of information security breaches on stock returns: Is the cyber crime a threat to firms? In Proceedings of the European Financial Management Meeting, Rome, Italy, 25–28 June 2014; pp. 1–12.
78. Das, S.; Mukhopadhyay, A.; Anand, M. Stock market response to information security breach: A study using firm and attack characteristics. *J. Inf. Priv. Sec.* **2012**, *8*, 27–55. [[CrossRef](#)]
79. Modi, S.B.; Wiles, M.A.; Mishra, S. Shareholder value implications of service failures in triads: The case of customer information security breaches. *J. Oper. Manag.* **2015**, *35*, 21–39. [[CrossRef](#)]
80. Schatz, D.; Bashroush, R. The impact of repeated data breach events on organisations' market value. *Inf. Comput. Secur.* **2016**, *24*, 73–92. [[CrossRef](#)]
81. Chen, Y.; Dong, F.; Chen, H.; Xu, L. Can cross-listing mitigate the impact of an information security breach announcement on a firm's values? In Proceedings of the 7th International Scientific Practical Conference "Innovative Technologies in Engineering", Yurga, Russia, 19–21 May 2016.
82. Martin, K.D.; Borah, A.; Palmatier, R.W. Data privacy: Effects on customer and firm performance. *J. Mark.* **2017**, *81*, 36–58. [[CrossRef](#)]
83. Sinanaj, G.; Zafar, H. Who wins in a data breach? A comparative study on the intangible costs of data breach incidents. In Proceedings of the Pacific Asia Conference on Information Systems (PACIS), Chiayi City, Taiwan, 27 June–1 July 2016; pp. 60–75.
84. Arcuri, M.C.; Brogi, M.; Gandolfi, G. How does cyber crime affect firms? The effect of information security breaches on stock returns. In Proceedings of the First Italian Conference on Cybersecurity, Venice, Italy, 17–20 January 2017; pp. 175–193.
85. Johnson, M.S.; Kang, M.J.; Lawson, T. Stock price reaction to data breaches. *J. Financ. Issues* **2017**, *16*, 1–12.
86. Abhishta, A.; Joosten, R.A.; Nieuwenhuis, L.J.M. Analysing the impact of a DDoS attack announcement on victim stock prices. In Proceedings of the 25th Euromicro International Conference on Parallel, Distributed and Network-based Processing, PDP 2017, St. Petersburg, Russia, 6–8 March 2017; pp. 354–362.
87. Rosati, P.; Cummins, M.; Deeney, P.; Gogolin, F.; van der Werff, L.; Lynn, T. The effect of data breach announcements beyond the stock price: Empirical evidence on market activity. *Int. Rev. Financ. Anal.* **2017**, *49*, 146–154. [[CrossRef](#)]
88. Hovav, A.; Han, J.Y.; Kim, J. Market reaction to security breach announcements: Evidence from South Korea. *Data Base Adv. Inf. Syst.* **2017**, *48*, 11–52. [[CrossRef](#)]
89. Patsakis, C.; Charemis, A.; Papageorgiou, A.; Mermigas, D.; Pirounias, S. The market's response toward privacy and mass surveillance: The snowden aftermath. *Comput. Secur.* **2018**, *73*, 194–206. [[CrossRef](#)]
90. Jeong, C.Y.; Lee, S.Y.T.; Lim, J.H. Information security breaches and IT security investments: Impacts on competitors. *Inf. Manag.* **2019**, *56*, 681–695. [[CrossRef](#)]
91. Rosati, P.; Deeney, P.; Cummins, M.; Van der Werff, L.; Lynn, T. Social media and stock price reaction to data breach announcements: Evidence from US listed companies. *Res. Int. Bus. Financ.* **2019**, *47*, 458–469. [[CrossRef](#)]
92. Chang, K.-C.; Gao, Y.-K.; Lee, S.-C. The effect of data theft on a firm's short-term and long-term market value. *Mathematics* **2020**, *8*, 808. [[CrossRef](#)]

93. Filbeck, G.; Swinarski, M.; Zhao, X. Shareholder reaction to firm investments in the capability maturity model: An event study. *Eur. J. Inf. Syst.* **2013**, *22*, 170–190. [CrossRef]
94. Dehning, B.; Richardson, V.J.; Zmud, R.W. The financial performance effects of IT-based supply chain management systems in manufacturing firms. *J. Oper. Manag.* **2007**, *25*, 806–824. [CrossRef]
95. Hendricks, K.B.; Singhal, V.R.; Stratman, J.K. The impact of enterprise systems on corporate performance: A study of ERP, SCM and CRM system implementations. *J. Oper. Manag.* **2007**, *25*, 65–82. [CrossRef]
96. Bener, A.B. Risk Perception, Trust and Credibility: A Case in Internet Banking. Ph.D. Thesis, London School of Economics and Political Sciences, London, UK, 2000.
97. Barber, B.M.; Lyon, J.D. Detecting long-run abnormal stock returns: The empirical power and specification of test statistics. *J. Financ. Econ.* **1997**, *43*, 341–372. [CrossRef]
98. Kothari, S.; Warner, J.B. Measuring long-horizon security price performance. *J. Financ. Econ.* **1997**, *43*, 301–339. [CrossRef]
99. Lyon, J.D.; Barber, B.M.; Tsai, C.L. Improved methods for tests of long-run abnormal stock returns. *J. Financ.* **1999**, *54*, 165–201. [CrossRef]
100. Hendricks, K.B.; Singhal, V.R. The effect of demand–supply mismatches on firm risk. *Prod. Oper. Manag.* **2014**, *23*, 2137–2151. [CrossRef]
101. Healy, P.M.; Palepu, K.G. Earnings and risk changes surrounding primary stock offers. *J. Account. Res.* **1990**, *28*, 25–48. [CrossRef]
102. Hertzfel, M.; Jain, P.C. Earnings and risk changes around stock repurchase tender offers. *J. Account. Econ.* **1991**, *14*, 253–274. [CrossRef]
103. Fargher, N.L.; Wilkins, M.S. Evidence on risk changes around audit qualification and qualification withdrawal announcements. *J. Bus. Financ. Account.* **1998**, *25*, 829–847. [CrossRef]
104. Clayton, M.C.; Hartzell, J.C.; Rosenberg, J. The impact of CEO turnover on equity volatility. *J. Bus.* **2005**, *78*, 1779–1808. [CrossRef]
105. Barberis, N.; Huang, M. Mental accounting, loss aversion, and individual stock returns. *J. Financ.* **2001**, *56*, 1247–1292. [CrossRef]
106. Xu, Y.; Malkiel, B.G. Investigating the behavior of idiosyncratic volatility. *J. Bus.* **2003**, *76*, 613–645. [CrossRef]
107. Goyal, A.; Santa-Clara, P. Idiosyncratic risk matters! *J. Financ.* **2003**, *58*, 975–1007. [CrossRef]
108. Ang, A.; Hodrick, R.J.; Xing, Y.; Zhang, X. The cross-section of volatility and expected returns. *J. Financ.* **2006**, *61*, 259–299. [CrossRef]
109. Bali, T.G.; Cakici, N.; Yan, X.; Zhang, Z. Does idiosyncratic risk really matter? *J. Financ.* **2005**, *60*, 905–929. [CrossRef]
110. Hsieh, S.J.; Jerris, S.I.; Kross, W. Quarterly earnings announcements and market risk adjustments. *J. Bus. Financ. Account.* **1999**, *26*, 313–336. [CrossRef]
111. Ashbaugh-Skaife, H.; Collins, D.W.; Kinney, W.R., Jr.; LaFond, R. The effect of SOX internal control deficiencies on firm risk and cost of equity. *J. Account. Res.* **2009**, *47*, 1–43. [CrossRef]
112. Lee, I.; Loughran, T. Performance following convertible bond issuance. *J. Corp. Financ.* **1998**, *4*, 185–207. [CrossRef]
113. Hendricks, K.B.; Singhal, V.R. An empirical analysis of the effect of supply chain disruptions on long-run stock price performance and equity risk of the firm. *Prod. Oper. Manag.* **2005**, *14*, 35–52. [CrossRef]
114. Ali, S.E.A.; Khurram, S. Impact of demographic and health factors on GDP growth of South Asian Countries. *Int. J. Acad. Res. Bus. Soc. Sci.* **2017**, *7*, 2222–6990.
115. Carhart, M.M. On persistence in mutual fund performance. *J. Financ.* **1997**, *52*, 57–82. [CrossRef]
116. Fama, E.F.; French, K.R. Multifactor explanations of asset pricing anomalies. *J. Financ.* **1996**, *51*, 55–84. [CrossRef]
117. Jegadeesh, N.; Titman, S. Returns to buying winners and selling losers: Implications for stock market efficiency. *J. Financ.* **1993**, *48*, 65–91. [CrossRef]
118. Cowan, A.R.; Sergeant, A.M. Interacting biases, non-normal return distributions and the performance of tests for long-horizon event studies. *J. Bank. Fin.* **2001**, *25*, 741–765. [CrossRef]
119. Bhagat, S.; Brickley, J.A.; Loewenstein, U. The pricing effects of interfirm cash tender offers. *J. Financ.* **1987**, *42*, 965–986. [CrossRef]
120. Dann, L.Y.; Masulis, R.W.; Mayers, D. Repurchase tender offers and earnings information. *J. Account. Econ.* **1991**, *14*, 217–251. [CrossRef]
121. Abergel, F.; Politi, M. Optimizing a basket against the efficient market hypothesis. *Quant. Financ.* **2013**, *13*, 13–23. [CrossRef]
122. Malkiel, B.G. The efficient market hypothesis and its critics. *J. Econ. Perspect.* **2003**, *17*, 59–82. [CrossRef]
123. Shleifer, A.; Vishny, R.W. The limits of arbitrage. *J. Financ.* **1997**, *52*, 35–55. [CrossRef]
124. De Bondt, W.F.; Thaler, R.H. Further evidence on investor overreaction and stock market seasonality. *J. Financ.* **1987**, *42*, 557–581. [CrossRef]
125. StarTribune. Target settles class-action suit over data breach claims for \$39 million. *StarTribune*. 7 January 2017. Available online: <https://www.startribune.com/financial-firms-target-settle-breach-claims-for-39-million/360051311/> (accessed on 13 December 2020).
126. Sidel, R. Home depot’s 56 million card breach bigger than target’s. *Wall Street Journal*. 18 September 2014. Available online: <https://www.wsj.com/articles/home-depot-breach-bigger-than-targets-1411073571> (accessed on 13 December 2020).
127. Khansa, L.; Cook, D.F.; James, T.; Bruyaka, O. Impact of HIPAA provisions on the stock market value of healthcare institutions, and information security and other information technology firms. *Comput. Secur.* **2012**, *31*, 750–770. [CrossRef]