Ali, S. E. A., Lai, F.-W., Aman, A., Saleem, M. F., & Hamad, S. (2022). Do Information Security Breach and Its Factors Have a Long-Run Competitive Effect on Breached Firms' Equity Risk? *Journal of Competitiveness*, 14(1), 23–42. https://doi.org/10.7441/joc.2022.01.02

Do Information Security Breach and Its Factors Have a Long-Run Competitive Effect on Breached Firms' Equity Risk?

▪ *Syed Emad Azhar Ali, Fong-Woon Lai, Ameenullah Aman, Muhammad Furquan Saleem, Salaheldin Hamad*

Abstract

A breach in information security (infosec) can materially impact a firm's long-term competitiveness. For publicly listed firms, an infosec breach can have a long-lasting effect on their competitive stock performance, including their equity risk. Despite its significance, past research has focused primarily on examining the short-term effect of infosec breaches while ignoring its long-term effect on the firm's equity risk. Therefore, in this research, we examined the long-run effect of 276 infosec breaches at publicly traded firms on equity risk from 2009 to 2018. We analyzed each firm's equity risk compared to its competitive control firms of similar sizes and performances for three years, from one year before to two years after the breach, using a one-to-one matching methodology. The univariate analysis of infosec breaches on equity risk indicated that breach firms have a 7% higher equity risk than competitive control firms. Additionally, the quantile regression analysis of the effect of infosec breach factors on long-run equity risk showed that the rise in equity risk is higher if the breach involves the compromise of confidential information and is a repeat breach for the same firm. The findings provide a valuable resource for investors, managers, and researchers interested in understanding the long-term relationship between infosec breaches and a firm's stock competitiveness.

Keywords: information security breach, equity risk, competitive advantage, one-to-one matching
JEL Classification: D53, G32

Received: December, 2021
1st Revision: February, 2022
Accepted: February, 2022

1. INTRODUCTION

With the extensive use of digital technology and the developing nature of digital assets, the number of infosec breaches has increased, putting businesses at risk and eroding their competitiveness. As a result, a resilient approach for infosec risk management is vital for organizational growth and can help a firm outperform the competition. Cybercriminals are among the many competitors but are not included in a competitive analysis because they are not direct business competitors. These hackers want to steal money, sensitive data, and password-protected information such as

credit card details. The reason hackers are considered competitors is because they are typically not one-person hacker bands but rather profit-driven business entities (Kolodgy, 2021). In today's competitive business climate, the presumption of a cybersecurity breach or its broader form, the infosec breach, has become the new norm (Njenga & Lowry, 2018; Olcott, 2019), and breaches are expanding in size and impact (De Groot, 2020).

When a firm suffers an infosec breach, it may sustain both tangible and intangible damages that impair future cash flows and overall competitiveness, including the stock market (Hovav et al., 2017; Smith et al., 2019). Measuring such competitiveness is challenging. Thus, several researchers have attempted to measure this effect (Sinanaj & Muntermann, 2013; Tweneboah-Kodua et al., 2018). Most of these studies' findings showed an unfavorable effect on competitiveness, as measured by the breached firm's market value. The semi strong efficient market hypothesis (EMH), according to which stock prices react quickly to new information, underpinned these studies (Fama, 1970). As a result, scholars have analyzed stock price behavior displaying an immediate analysis of a firm's stock competitiveness. Whereas short-run analysis helps gauge a firm's short-term competitiveness to an event, long-run analysis is required to assess the actual economic impact on the firm's competitiveness. Studies on this issue have not provided a clear answer as to whether a breach will affect stock competitiveness in the long term.

An infosec breach can have a long-run effect on business operations, especially on investors in the stock market. For instance, the risk of infosec to operations, profits, and competitiveness is growing for many firms. The time required to identify and contain an infosec breach has increased from 257 days in 2017 to 282 days in 2020, with projected response costs ranging from about USD 1 million per organization (IBM & Ponemon, 2020). This reflects the increasing complexity of infosec breaches, which requires firms to commit more time and resources to counteract. The costs might linger for years because detecting and containing a breach are now slower. A firm's breach may necessitate assistance from cybersecurity, public relations, and legal firms, all of which add to the post-event cost. In addition to helping restore service, operations, and morale, brand harm and stakeholder confidence can take months to heal (McAfee, 2021). These are anticipated to have a long-term impact on the firm's operational excellence and competitiveness, particularly in the stock market. Second, firms are hesitant to provide signals that disclose complete details of a breach in their initial announcement. If a company has not detected a breach, it cannot report it. Even if a breach is detected, it still might not be reported. In recent years, incidents of infosec breaches have occurred in which the details of the breach have been revealed months after the initial breach announcement. For example, in July 2019, Equifax was fined USD 700 million by the Federal Trade Commission and the Consumer Financial Protection Bureau for concealing material details of a massive data breach that occurred in 2017. Similarly, the SEC fined Yahoo! USD 35 million in 2018 for allegedly misleading investors by failing to report a 2014 personal data breach affecting over 500 million user accounts (Rutta & Diamond, 2018). According to a report by McAfee (2021), only 26% of organizations that experienced security incidents shared real-time information about the most severe incident with customers and investors. From a stock market perspective, disclosures after infosec breaches by the firms and other parties provide signals to stock investors for long-run decision-making, thus affecting overall firm risk (Aman et al., 2021). How infosec breaches affect equity risk is critical

to understand because they can affect stock competitiveness (Ali et al., 2020). This may increase the firm's cost of capital and deter investors from investing in a stock.

The factors contributing to abnormalities in a firm's stock competitiveness as measured by equity risk are critical to investigate. Therefore, in this study, we also examined the relationship between infosec breach factors and long-term equity risk abnormalities. We assert that an infosec breach can have a long-term detrimental effect on equity risk, with varying magnitudes depending on the contributing infosec breach factors. With an underpinning of signaling theory, the magnitude of abnormality in equity risk is determined by the signals gained by investors after an infosec breach (Helm & Mark, 2007; Ray et al., 2011). Signaling factors revealed after an infosec breach may influence the extent of the abnormality in the equity risk. The nature of the breach may be one factor. That is, the reaction of an investor (receiver) depends on whether the confidential information of the breached firm has been compromised (confidential/non-confidential) (Chang et al., 2020; Yayla & Hu, 2011). Similarly, an investor's reaction may differ depending on whether the firm has been breached for the first time or repeatedly (repeat/no-repeated) (Chen et al., 2011; Hovav et al., 2017). Additionally, a breach affecting a large conglomerate may have different ramifications for investors than a breach affecting a conglomerate's subsidiary (conglomerate/subsidiary) (Bose & Leung, 2014; Smith et al., 2019). Finally, the industry in which a breached firm operates may have a varied impact on investors (Hovav et al., 2017), mainly if the breached firm is in the financial sector (financial/non-financial). Considering this scenario, we aimed to achieve the following research objectives (ROs) in this study:

1. To evaluate the long-run effect of infosec breaches on equity risk.
2. To examine the role of infosec breach factors in determining the magnitude of long-run abnormalities in equity risk (stock volatility) following an infosec breach.

Section 2 reviews the literature on the effect of infosec breaches on equity risk and discusses the theoretical foundations upon which the research hypotheses were developed for this research. Section 3 outlines the long-term equity risk forecasting methodology. Section 4 presents the results on the long-run effect on equity risk along with a discussion given the study's ROs and the findings of other studies. Section 5 concludes this study by first describing the theoretical and practical contributions and then identifying the limitations and future research opportunities in this field.

2. LITERATURE REVIEW AND HYPOTHESIS DEVELOPMENT

An influential research group focused on the market implications of disclosures linked to infosec breaches underpinning the EMH and the methodology of an event study (Chang et al., 2020; Smith et al., 2019). The event study tested the EMH by tracking and analyzing major post-announcement stock price changes. Researchers have used this methodology to study infosec breach events such as denial-of-service attacks (Rosati et al., 2019; Smith et al., 2019), virus attacks, and software vendor vulnerability announcements (Telang & Wattal, 2007). These researchers all focused on the short-term effects of breaches while disregarding their long-term consequences.

In the current study, we used signaling theory to account for the long-term influence of infosec breaches on a firm's stock competitiveness as manifested by its equity risk (Spence, 1978, 2002). According to the theory, a firm's products or services may signal customers, allowing them to make indirect judgments based on available information. An infosec breach sends a strong signal to investors about the resilience of a firm's infosec system and its prospects. To begin, an infosec breach raises the risk of online transactions (Pavlou et al., 2007), hence affecting the firm's future cash flows and stock competitiveness. Second, investors' subsequent actions will be based on the infosec breach signals shared by breached firms, which will impact possible litigation expenses from customers (Gordon et al., 2010). Prior findings on patent infringement indicated that litigation may hurt the market value of defendants (Raghu et al., 2008). Third, an infosec breach may attract other adversaries or competitors who prefer firms with lax security measures. Lower security and privacy assurance levels may create transactional uncertainty and reduce purchase conversion (Özpolat et a., 2013). Finally, a security breach may exacerbate market information asymmetry due to the breached firms' restricted disclosure. Higher information asymmetry can affect market returns and lemon market difficulties (Gordon et al., 2010). Thus, the events can be considered a signal for investors. Investors' expectations of a company's future performance and outlook are revised after a breach, causing a market reaction to the firm's stock competitiveness.

The ramifications for the firm's long-term competitiveness, particularly in the stock market, are a common concern for researchers because the term long-run firm's stock competitiveness refers to the degree of change in stock price from one to three years after an occurrence. Long-run firm stock competitiveness is influenced by the scenarios that surround an event. Similarly, an infosec breach can have long-term effects on a firm's finances and stock competitiveness. However, most researchers have focused on infosec breaches' short-term stock competitiveness.

To the best of our knowledge, only two recent studies (Ali et al., 2021b; Chang et al., 2020) have explored the long-run effect of infosec breaches on a firm's stock competitiveness. Chang et al. (2020) employed a traditional event study methodology by comparing the breached firms' performance to that of the market. According to Barber & Lyon (1997), Kothari & Warner (1997), event study methodology prevents determining the actual economic impact and test statistics of reported abnormal returns. Cross-sectional dependency is the leading cause of misspecification because sample firms' long-run market prices generally overlap. Positive or negative cross-sectional dependency skews test outcomes. According to the current simulations, one-to-one matching of abnormal returns produces well-specific tests (Barber & Lyon, 1997; Hendricks & Singhal, 2014; Lyon et al., 1999). According to the one-to-one matching approach, each sample firm's performance is compared to that of a competitive matching firm with a similar size and prior performance. Considering this research gap, Ali et al. (2021b) employed a one-to-one matching methodology; however, their study was limited to 73 breach events. Furthermore, the analysis was confined to only one year. As such, in this study, a framework was created using a robust and reliable one-to-one matched methodology. Additionally, equity risk for three years was examined, from one year before to two years after the breach. A larger sample of 276 breach events was used. To the best of the author's knowledge, the literature does not provide an adequate answer regarding the long-run effect of infosec breaches on equity risk.

2.1 Infosec breaches and long-run equity risk of firms

Understanding how business events and their opinions affect equity volatility is critical given the economic ramifications. An infosec breach event was proved, in past studies, to substantially affect the stock market prices of breached firms. In addition to the consequences on stock prices, an infosec breach can remarkably impact the level of equity risk faced by firms and their investors. Regarding making financial investment decisions, equity risk is a critical factor to consider. According to our knowledge, only a few researchers have analyzed the impact of an infosec breach on equity risk. Hinz et al. (2015) and Tweneboah-Koduah et al. (2020) have explored the influence of infosec breaches on equity risk. However, their research was limited to a short time frame. In the long run, firms that are found to be vulnerable to infosec breaches may be perceived as systematically more vulnerable to further assaults, and investors may demand larger compensations for this exposed risk. Further, infosec breaches are predicted to adversely affect investors' expectations about a firm's future cash flows, increasing the equity risk. Taking the above into consideration, the first hypothesis as developed as follows:

H1: Infosec breaches augment the long-run equity risk of breached firms ($\sigma 2e$).

The literature provides no guidance on the ideal time frame for assessing post-announcement equity risk with reasonable assumptions. The literature covers a period of one to five years. However, using more than two years of abnormal returns create misspecified and unbiased test statistics (Huang, 2012; Kothari & Warner, 1997). The event determines the suitable timeframe for examination and the scholars' clear choice (Huang, 2012). This post-event study is consistent with that of Hendricks & Singhal (2005, 2014), who examined complex incidents that cannot be appraised in the absence of additional information. We estimated equity risk following the disclosure of an infosec breach over three years, commencing one year prior to the incident and ending two years after the breach. This demonstrates the negative implications of infosec breaches and any constructive effects of corrective actions. Overall, we examined the SD of stock returns over three distinct periods, including the pre- and post-breach periods of one year, between the first and second years following the breach, and over three years beginning one year before and ending two years following the breach.

2.2. Infosec breach factors and long-run equity risk

An infosec breach signals a firm's information system's vulnerabilities based on signaling theory. Investors' reactions may vary based on the factors that created the infosec breach. In addition to the long-term effect of an infosec breach on equity risk, these factors must be examined. Elements connected with infosec breaches can help explain the magnitude of abnormalities in a firm's stock competitiveness (Yayla & Hu, 2011). Among the factors are the characteristics of the infosec breach or attack (Arcuri et al., 2017; Bose & Leung, 2014), firm characteristics (Goel & Shawky, 2009; Rosati et al., 2017), and industry characteristics (Pirounias et al., 2014; Yayla & Hu, 2011). As a result, the following hypothesis was constructed for each infosec breach factor.

H2: Infosec breach factors affect the magnitude of abnormalities in long-run equity risk.

H2 was further divided into four sub-hypotheses, H2A, H2B, H2C, and H2D, based on the four factors of infosec breach conceptualized and examined in this study. These factors can

also be demonstrated by signaling theory and integrated into a signaling framework to aid in comprehending investor decision-making. These factors can be classified as the signaler (the party disclosing the new information), signal (the information being disclosed), receiver (the party receiving/interpreting the signal and their response), and signaling environment (the context in which all of this occurs) (Connelly et al., 2011; Hamad et al., 2020). We used these classifications to identify infosec breach factors that may affect equity risk in the event of an infosec breach. We argue that the net effect of infosec breaches on the investor (signal receiver) is contingent on the following factors: (1) the signal content, i.e., the disclosed infosec breach; (2) the signaler, i.e., the firm in question; and (3) the signaling environment surrounding the infosec breach.

The nature of the breach serves as the signal content and is thus conceptualized in H2A (Arcuri et al., 2017; Bose & Leung, 2014). Firm characteristics (e.g., repeated breaches to a firm and firm's ownership structure) function as a signaler (Goel & Shawky, 2009; Rosati et al., 2017) and are conceptualized in H2B and H2C. The breached firm's industry serves within the boundaries of a signaling environment and is conceived in H2D (Bose & Leung, 2014; Pirounias et al., 2014; Yayla & Hu, 2011).

Customers, stockholders, and other business stakeholders are more concerned about the theft of confidential information than denial-of-service attacks, virus attacks, or other infosec breaches (Bose & Leung, 2014; Hovav et al., 2017). The majority of the researchers have focused on the short-term effects of an infosec breach. A short-term examination of an infosec breach event cannot reveal its actual impact on a firm's stock competitiveness. For instance, in the case of SONY, the number of breaches escalated following the initial notice, owing to the attacker's opportunistic stealing behavior and the access gained to the organization's information system (IS), resulting in the compromise of additional confidential information (Goode et al., 2017). As a result, long-term equity risk is projected to be higher when confidential information is compromised. The study's RO2 suggests that a security breach that compromises confidential information will serve as a warning to investors, increasing long-term equity risk.

H2A: Long-run abnormal equity risk is higher for infosec breaches that compromise confidential information than for other types of breaches.

The first breach is seen differently than a second, third, or additional breach. Simultaneously experiencing multiple breaches signals a great deal to investors about a firm's infosec resilience. As a result, they are likely to punish firms that fail to protect sensitive data. Suppose the market's reaction to a repeated incident is the same. In that case, this suggests investors are seeking long-term signals that can help them create trust in the market. Investors who penalize firms for failing to improve in infosec may show indifference or even preference in the long run. As a result, if the same firm is repeatedly breached, the effect on equity risk must be assessed. Some attempts to understand this relationship have been made by Gatzlaff et al. (2010); Schatz & Bashroush (2016). Despite the importance of long-term analysis (highlighted earlier), both of these attempts solely focused on the short-term firm stock performance. As a result, the following sub-hypothesis was formulated:

H2B: Long-run abnormal equity risk following an infosec breach is higher for firms that experience repeated breaches.

A breached firm's ownership structure also provides a distinct signal. In the event of an infosec breach, a firm's ownership status may influence investor reaction. Conglomerates with subsidiary firms are more likely to diversify risk (Du et al., 2021). The implications of an infosec breach in a conglomerate's subsidiary may be less severe. The status of the subsidiary has a mitigating effect in the case of data breach notifications (Bose & Leung, 2014) and DoS attack announcements. The rationale is that investors pay more attention to news that affects a conglomerate's overall profitability and competitiveness than to information that influences a single subsidiary's profitability. Because of the risk diversification, whereas infosec breaches may have long-term adverse effects on the target firm, they have less impact on a subsidiary of a more prominent firm. Due to these signals, equity risk may be higher when a conglomerate is breached. Thus, the following sub-hypothesis was proposed:

H2C: Long-run abnormal equity risk is higher if the breach directly targets a conglomerate firm than if it targets a conglomerate firm's subsidiary.

As a component of the signaling environment, the industry plays a role in signaling to investors after an infosec breach. Cybercriminals target financial organizations because they have access to sensitive data, including client PINs, social security numbers, and credit card details. Among all the major industries, firms in the financial industry spend the most time identifying and managing infosec breaches at 233 days (IBM & Ponemon, 2020). Additionally, the average cost of an infosec breach is substantially higher in the finance industry than in other industries (Bissell & Ponemon, 2019). The cost of a breach exhibits the threat of cybercrime to financial services firms. Moreover, financial firms face higher legal, financial, and client risks than firms in other industries (Bouveret, 2018). Thus, breaches in the financial sector can lead to customer distrust and possibly legal action from customers and regulators, as was the case for Equifax (Fung, 2018). So, an infosec breach in the financial industry will have stronger impacts on future cash flows and stock prices than in other industries. The cumulative effect of all of these aspects can substantially enhance the long-term equity risk of a financial firm compared to other types of firms. It may impair long-term equity risk. As a result, the following sub- hypothesis was constructed:

H2D: Long-run abnormal equity risk after an infosec breach will be higher for financial sector firms than non-financial sector firms.

3 METHODOLOGY AND DATA

The methodology and estimation procedures used in this study are different from those used in event studies to assess the short-term effect of events on firm stock competitiveness. Event studies frequently produce skewed estimates of eventual economic impact and test statistics (Barber & Lyon, 1997; Kothari & Warner, 1997). This study's findings are based on modern, more precise approaches that were used in a few studies (Ali et al., 2021a; Hendricks & Singhal, 2005, 2014)

3.1. Sample selection:

The sample was compiled using web data sources such as The Privacy Rights Clearinghouse (PRCH) and the Identity Theft Resource Center (ITRC). Previously, researchers used these data sources (Richardson et al., 2019; Rosati et al., 2019). Event denotes the date of a security breach disclosure. The breadth of an infosec breach varies and may contain names, addresses, dates of birth, passwords, and credit card information. In this study, the inclusion criteria of all infosec breach announcements from a firm were:

1. The firm was listed on one of the U.S. stock markets (NYSE or NASDAQ).
2. The firms had provided data to the Center for Research in Security Prices database.
3. The firm had traded for a year prior to the infosec breach.
4. The firm had no other infosec breaches in the two years before and after the breach.
5. When the breach occurred on an unlisted subsidiary firm, the parent company was tracked.
6. The firm had a book value greater than zero.

Obtaining a large enough event sample size for statistical analysis has challenged event study scholars. This challenge involves identifying relevant press releases that influenced investor trading. As per the systematic literature review by Ali et al. (2021a), 90% of studies that examined the effect of infosec breaches on firm stock competitiveness used a sample size of approximately 200 events. The sample data for this study were obtained from the PRCH and ITRC, which allowed for the collection of 763 breach events from 2009 to 2018 (Table 1). The samples were then screened for long-term analysis using the above criteria. To begin, 245 samples were discarded because the breached firm was not publicly traded. Another 100 samples were removed because they occurred within two years after an infosec breach at the same firm, restricting long-term analysis. Next, 100 samples were excluded due to a lack of data for a two-year analysis. Lastly, 37 samples were eliminated for failing to meet the inclusion criteria (Section 3.1). For instance, firms had a book value of less than zero. Using this procedure, 276 breaches were used to gauge long-term equity risk. Figure 1 depicts the industry classification for the breach events included in our final sample.

Tab. 1 – Sample selection criteria. Source: own research

Year	Sample size	Non-publicly listed firms	Event period < 2 years	Insufficient data	Book value < 0	Finalized sample firms
2009	55	19	5	13	2	16
2010	65	18	11	14	5	17
2011	69	18	15	7	5	24
2012	71	25	7	8	3	28
2013	79	32	6	5	4	32
2014	77	25	7	7	3	35
2015	71	27	6	8	3	27
2016	92	29	19	9	4	31

2017	105	27	18	15	5	40
2018	79	25	11	14	3	26
Total	763	245	105	100	37	276

3.2. Assessing the long-run equity risk:

The main challenge in this long-term stock market research was predicting abnormalities for the firms in our sample. In this situation, abnormal equity risk is the difference between a sample firm's equity risk and a competitive benchmark risk over a period. After controlling for the indicated variables, whatever is unexplained is considered abnormal and can be linked to the event. The literature provides different views on measuring long-term abnormality (Barber & Lyon, 1997; Fama, 1998). The present consensus is that long-run abnormalities must be determined after controlling for size, market-to-book (M/B) ratio, and previous performance through the use of matched sampling methodology (Barber & Lyon, 1997; Lyon et al., 1999).

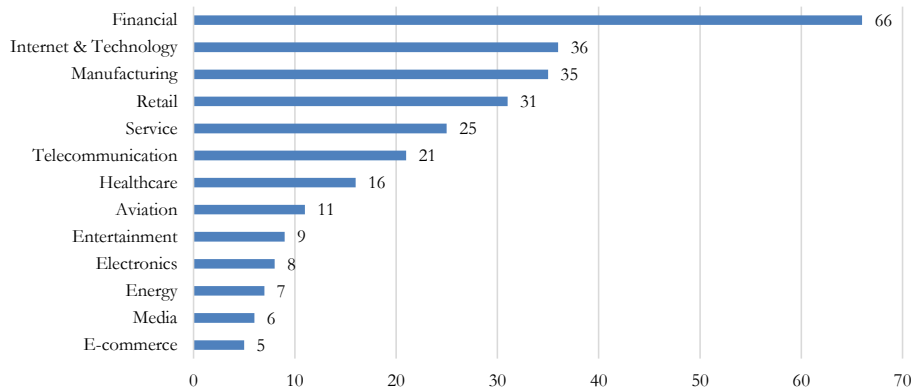

Fig. 1 – Number of sample breach events across different industries. Source: own research

This methodology has been applied in many previous studies (Ali et al., 2021b; Richardson et al., 2019) and appeared to be most appropriate for testing the hypotheses. According to this methodology, each sample firm was matched to a competitive control firm of similar size and performance. Then, two one-to-one samples (control firms) were established as follows:

1. Choosing a control firm in the same industry that is 70% to 130% of the asset size of the sample firm (size-matched).

2. Choosing a control firm from the same industry as the sample firm with an M/B ratio of 70% to 130% (performance-matched).

Equity risk (i.e., equity volatility) can be expected to change after an infosec breach is reported. Additionally, some information may leak about market-wide infosec breaches. Infosec breaches may also affect information risk, financial leverage, and operational levers. So, volatility fluctuations were studied before and after an infosec breach. The pre-event period (days -259 to -10) was used to assess volatility variations. The post-announcement volatility fluctuations were investigated to determine if they were temporary or irreversible. Volatility is the SD of the

portfolio's abnormal returns over time. A minimum of 125 daily returns should be accessible in one year to predict SDs. The SD is a financial statistic that shows the investment's historical volatility compared to the average return.

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

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

We compared the percentage changes in our sample firms' equity standard deviations with the competitive control firms using matched sampling methodology. Thus, each sample firm's equity risk was matched with two similar competitive control firms. This controlled for industry-matched size and performance. The study calculated percentage increases in volatility as follows:

%⊿ volatility=%⊿ in volatility of sample firm -%⊿ in volatility of control firm (2)

Once the equity risk (i.e., abnormal stock volatility) was analyzed through equation 2, its significance was tested through parametric (t-test) and nonparametric tests (Wilcoxon signed-rank test). The test results finally revealed the acceptance or rejection of H1 for this study. To collect findings over time, we calendared each entity's occurrence in our sample. The day of the announcement was the day '0', and the next trading day was day '1' the day before was day -1, and so on. Abnormal equity SDs were analyzed for three years, from one year before to two years after the event. A year has 250 trading days. Additionally, a two-week term (10 trading days) was deducted from both sides. This ensured that estimates of equity SDs were not skewed by abnormal trading activity leading up to the event. As exhibited in Table 2, we evaluated stock volatility over three years, beginning one year before and after the breach.

Tab. 2 – Time mapping to compute equity SDs. Source: own research

	Post-event period		
	Year -1 to +1	Year +1 to +2	Year -1 to +2
Stock volatility (in days)	-259 to +259 days	+260 to 509 days	-259 to 509 days

The equity SDs were computed for three separate windows: 1) one year prior to and following the event (Equity SD-1,+1); 2) between one and two years following the event (Equity SD+1,+2); and 3) between one and two years following the event (Equity SD-1,+2). Parametric and nonparametric tests were used to assess the statistical significance of these equity SDs and H1.

3.3. Cross-sectional regression for infosec breach factors on equity risk:

For testing H2, infosec breach factors were regressed at windows where equity SDs were significant. Time frame, breached firm size, and M/B ratio were all unrelated control variables. The natural log of the breached firm's total assets reported in the year of disclosure determines the firm's size (Bose & Leung, 2014, 2019). The timeframe was ten years, from 2009 to 2018, so it had a maximum value of ten (the year 2018) and a minimum value of 1 (the year 2009) (Ali et al., 2021a; Chang et al., 2020). Each sample firm was paired with a competitive control firm. Controlling the sample firms' M/B was crucial because M/B determines their performance

(Barber & Lyon, 1997; Lyon et al., 1999). The hypothesized variables for infosec breach factors are were 1 and 0. Table 3 shows the operationalization of these dummy variables, which is in line with the infosec literature, where code 1 denotes dimension that is expected to create a higher abnormality in equity risk. Quantile regression (QR) was used instead of ordinary least squares (OLS) to assess H2A–H2D because it is robust to the non-normality of error terms and outliers and minimizes cross-sectional and cross correlational heteroskedasticity (Bose & Leung, 2019; Huang et al., 2017).

Tab. 3 – Operationalization of study variables. Source: own research

Factor	Variables	Source	Formulas	Reference
Nature of Breach	Independent dummy variable	Content analysis of the news source	"1" if the breach has compromised the confidential information, otherwise "0."	(Hovav et al., 2017; Malhotra & Malhotra, 2011)
Repeated Breach			"1" if it is a repeated breach to a similar firm; otherwise, "0".	(Modi et al., 2015; Schatz & Bashroush, 2016)
Breached firm's ownership structure			"1" if the breached firm is a "conglomerate" and "0" if it is "subsidiary.	(Bose & Leung, 2014, 2019)
Breach firm's industry			"1" if the breached firm is from the financial industry; otherwise, "0".	(Bose & Leung, 2014)

4. RESULTS AND DISCUSSION

The correlations of all study variables are exhibited in Table 4. In line with the second research objective, a positive correlation was found between some infosec breach factors and the equity SDs. However, a comprehensive investigation of these relationships was necessary before drawing any conclusions. Tables 5 and 6 provide comprehensive details of these relationships.

Tab. 4 – Person correlation matrix between hypothesized and control variables. Source: own research

Variables	Equity SD-1,+1	Equity SD+1,+2	Equity SD-1,+2	Nature of breach	Repeated breach	Breach firm's ownership	Breach firm's industry	Time frame	Firm size	M/B
Equity SD-1,+1	1									
Equity SD+1,+2	-.143	1								
Equity SD-1,+2	.750**	.318**	1							

Nature of breach	.380**	-.074	.384**	1						
Repeated breach	.297**	.006	.389**	-.082	1					
Breach firm's ownership	-.126	.016	-.025	-.023	0.01	1				
Breach firm's industry	.086	-.062	.488**	-.176*	.103	-.085	1			
Time frame	.221**	-.011	-.25**	.195**	-.184*	.206**	-.097	1		
Firm size	-.046	.010	-.053	.018	.118	.038	-.112	.118	1	
Market-to-Book	.042	-.039	.047	-.006	-.093	-.068	-.024	-.07	.00	1

Notes: **Correlation is significant at the 0.01 level (2-tailed). *Correlation is significant at the 0.05 level (2-tailed).

To achieve RO1, we examined the long-term equity risk of breached firms from 2009 to 2018. To evaluate the equity risk of sample firms following the disclosure of an infosec breach event (year t = 0), the sample firm's equity SD was compared to that of a matched control firm. During the pre- and post-event period, the average change in equity $SD_{-1,+1}$ of sample firms compared to size-matched competitive control firms was positive. The mean abnormal change in equity SD was 8%, significant at the 5% level (t=2.475). In contrast, the Z-statistic for the Wilcoxon signed-rank test was 2.425. However, the change in equity risk was insignificant for equity SD+1,+2 (t=1.068). A substantial rise in equity risk was revealed in the cumulative period of three years (i.e., equity $SD_{-1,+2}$). Therefore, H1 was supported. The results for performance-matched competitive control firms were analogous to those of size-matched competitive control firms. Accordingly, further analysis and discussion centered on the size-matched control group.

Tab. 5 – Evidence for abnormal equity risk for sample breached firms when matched with size-control and performance-control firms at $SD_{-1,+1}$, $SD_{+1,+2}$ and $SD_{+1,+2}$. Source: own research

Performance statistics of changes in equity standard deviation (σ_e)	Time period		
	Equity $SD_{-1,+1}$	Equity $SD_{+1,+2}$	Equity $SD_{-1,+2}$
Relative to the size-matched control sample			
Mean abnormal change in SD	0.0801	0.0274	0.0768
t-statistica	**2.475***	1.068	**2.330***
Z-statisticb	**-2.42***	-0.378	**-2.558***
Relative to the performance-matched control sample			
Mean abnormal change in SD	0.1452	-0.1099	0.1705
t-statistica	**3.595***	-1.184	**3.92***
Z-statisticb	**-2.45***	-0.984	**-3.352***

a. Parametric t-test, significant at the level of 5% b. Non-parametric Wilcoxon signed rank test
*significant at the level of 5%

The higher equity risk revealed during these periods may have led to negative abnormal returns, as witnessed previously (Ali et al., 2021b; Chang et al., 2020). The equity risk outcomes are noteworthy for various reasons: First, when infosec breaches were publicly disclosed, equity risk significantly increased. Second, the increase in equity SDs prior to and during the infosec breach was not the result of a nonstationary SD range. SDs did not significantly differ between one and two years following the event. Finally, no temporary increase occurred in equity risk over the one year prior and following the infosec breach incident, as the risk did not diminish in the months following. Breach of infosec increased the risk to the firm and, as a result, the equity risk in the months ahead. Increased equity risk may also imply that sample firms' cost of equity will increase by 7% compared to controls. This will reduce the equity value of sample firms by 7%. Using SONY as an example, an infosec breach event would result in a market value loss of USD 293 million per year after the occurrence and a total loss of USD 937 million two years later.

Considering RO2, infosec breach factors were regressed on equity risk when it was significant: equity $SD_{(-1,+1)}$ and equity $SD_{(-1,+2)}$. Based on these results, the hypotheses connected with RO2 were assessed, namely H2A–H2D. The infosec breach factors were initially regressed using the OLS method. However, the regression functions failed to fully satisfy the OLS assumptions. Following the procedure of similar studies, QR was used. The QR results for equity $SD_{(-1,+1)}$ and equity $SD_{(-1,+2)}$ are shown in Table 6. The adjusted r-square values were 26% and 29%, respectively, implying that about 26-29% of the change in the conditional median in equity $SD_{(-1,+1)}$ and equity $SD_{(-1,+2)}$ was related to the infosec breach factors included in the model. The significance level for the quasi-LR statistic was less than 0.05, indicating that the models were stable.

Tab. 6 – Quantile regression results for infosec breach factors on Equity $SD_{-1,+1}$ and Equity $SD_{-1,+2}$. Source: own research

Factors	Equity $SD_{(-1,+1)}$	Equity $SD_{(-1,+2)}$		
	Coefficients	t	Coefficients	t
Constant	0.120206	1.210587	0.036925	0.301254
Nature of breach	**0.11307***	**2.61710***	**0.128885**	**2.46792***
Repeated breach	**0.16949***	**3.79897***	**0.139917**	**2.32296***
Breach firm's ownership structure	-0.002709	-0.066752	0.016333	0.305704
Breach firm's industry	0.027435	0.561417	0.031479	0.444082
Firm size	-0.004477	-0.259737	-0.004371	-0.212639
Timeframe	-0.015972	-2.14619*	-0.022215	-2.32812*
Market-to-book ratio	9.26E-05	0.007325	-0.003165	-0.213375
Prob (Quasi-LR stat)	0.000000		0.000000	
Adjusted R-square	0.2614		0.2893	

*significant at the level of 5%

Common infosec breach factors were found to be significant in determining the long-term equity SDs within one year before and after a breach (i.e., Equity $SD_{-1,+1}$) and in the cumulative period of one year before the breach to two years after the breach (i.e., Equity $SD_{-1,+2}$). The nature

of the breach was significantly positive (t=2.67, t=2.46) for Equity $SD_{-1, +1}$ and Equity $SD_{-1, +2}$,. Therefore, H2A was strongly supported. This implies that the breached firm's stock will be at higher risk when compromised by a breach affecting its confidential information. These findings are consistent with earlier research demonstrating how investors' confidence is influenced due to a firm's confidential information being compromised (Das et al., 2012). Researchers have studied this effect on the short-term horizon. In contrast, this analysis extends prior conclusions by arguing that an increase in equity risk caused by a breach of a firm's confidential information will occur in the short and long terms. Additionally, these findings imply that investors do not provide leverage to firms after a breach of confidential or sensitive information in the long run. On the contrary, investors may continue to offer leverage to firms when their ISs experience a breach of integrity or availability, as they are not directly involved in the loss of sensitive information or other major information assets (Bose & Leung, 2014; Hovav et al., 2017). Additionally, a breach of confidential information may result in the loss of additional consumers and a disproportionately higher legal liability, thereby exacerbating the incident's long-term effect (Ali et al., 2021b; Chang et al., 2020). Hence, a security breach of confidential information sends a strong signal to investors. As a result, increased abnormality in investors' long-run equity risk can be projected when a breach involves compromising confidential information.

Repeated breaches for the same organization (t = 3.79, t =2.32) were also significantly positive for Equity $SD_{-1,+1}$ and Equity $SD_{-1,+2}$. We can infer that if breaches repeatedly occur for the same firm, its stock will be at higher risk. Therefore, H2B was supported. This means that the increase in equity risk associated with infosec breaches will be markedly higher if a firm is repeatedly the victim of breaches. Additionally, the results indicate that repeated breaches at the same firm send an exceedingly negative signal to investors compared to when a firm is breached for the first time. As a result, investors will be more punitive of firms that fail to learn from previous breaches and establish an IS resilient to the risk of infosec breaches. These findings corroborate those of Gatzlaff & McCullough (2010); Schatz & Bashroush (2016), who evaluated the short-term effect of repeated breaches. The current study's findings indicate that the negative effect of a repeated breach lasts longer than that of an initial infosec breach on a firm.

No significant evidence was found as to a breached firm's ownership structure on equity SD on either of the timelines (t= -0.06, t= 0.35). Hence, H2C was rejected. A statistically insignificant association was found between the breached firm's ownership structure and long-run equity risk. The conclusion is that investors, in penalizing the breached firm, make no distinction between conglomerate and subsidiary firms. As a result, investors' reactions to an infosec breach event will be independent of the firm's ownership structure. These findings contradicted those of Bose & Leung (2014) when they examined the effect of infosec breaches on short-run market value. From the current study, it can be concluded that the negative effect of an infosec breach may endure only in the short term for a conglomerate and not in the long term for either the conglomerate or subsidiary firm. Thus, investors do not differentiate the negative effects of an infosec breach based on the firm's ownership structure as a conglomerate or subsidiary in the long run.

Finally, the breach effect concerning the breached firm's industry was also insignificant. This implies that equity risk did not differ between the breached firms' industries (t= 0.56, t= 0.44).

Therefore, H2D was rejected. Additionally, it was established that investors, when penalizing a breached firm, make no distinction between its industry classification as financial or non-financial. No connection was found between the industry in which the breach occurred and the long-term equity risk. This is also consistent with the findings of prior research, which indicates that the effect of infosec breach on firm stock performance is independent of the breached firm's industry (Acquisti et al., 2006; Kannan et al., 2007). Overall, the study's findings imply that an infosec breach has a long-term, unfavorable effect on equity risk if a firm is a continued victim of breaches that compromises its confidential information.

5. CONCLUSION

By concluding that infosec breaches have a long-term equity risk effect, the current study provides two contributions to signaling theory: by widening its reach to encompass long-term analysis and by deepening the theory in unfavorable situations such as infosec breaches. Thus, a new link between infosec breaches and long-term equity risk was revealed in this study. The current contributions may open new research possibilities by examining the effects of an infosec breach on other long-run measures of a firm's competitiveness. This study further contributes to the signaling theory by identifying antecedent factors that influence the value of a signal in the infosec context. Abnormalities in equity risk show that signal and signal factors play a crucial role in shaping the receiver's reaction. Concerning signal content factors, it was discovered that breaching confidential information has a more significant effect on long-term equity risk than compromising nonconfidential information. If the signaler (i.e., the firm) has been compromised several times, the adverse effect on the receiver (i.e., the investor) is worse. This has implications for signaling theory and the long-term relationship between infosec breaches and equity risk.

Our findings of long-run equity risk are essential for risk managers for several reasons. First, managers value long skyline estimates; they gradually broaden their view on a firm's competitiveness concerning the stock market. The timeframe of abnormal equity performance was highlighted here, the extent to which it continues, and whether firms swiftly recover from infosec breaches. Second, the results show that breached firms incur higher equity risks than competitive control firms. Infosec breaches may increase a firm's financial and operational leverage. As a result, firms can lower financial leverage by raising equity or retiring debt. Our findings may help a firm's competitors (i.e., experienced hackers and other cyber experts) identify the most vulnerable firms. These types of unforeseen effects are rather typical in infosec studies.

The current study has some limitations. First, the study exclusively included publicly listed firms in the U.S., where the most stringent data breach reporting rules exist. Other countries' security breach notification regulations are in their infancy. Our findings currently only apply to U.S.-based firms. However, future research may look at breached firms beyond the U.S. when other countries develop infosec breach disclosure laws. Second, the classification of infosec breach factors was built based on a content analysis of news. A content analysis is a subjective procedure that incorporates researcher bias. Future research should examine the long-term effect of various types of breach incidents, such as phishing, advanced persistent threat, and computer virus infections, on a firm's stock competitiveness. Finally, further research might integrate security

breach and security investment: how security investment plays a role in improving the firm's competitiveness after an infosec breach. To conclude, the ramifications of infosec incidents on stock competitiveness are substantial, severe, and lasting. However, little research on the subject has been conducted. As a result, the field is amenable to novel research approaches that may aid a firm in sustaining a competitive edge in the digital era.

References

1. Acquisti, A., Friedman, A., & Telang, R. (2006). Is there a cost to privacy breaches? An event study. Paper presented at the In: 27th International Conference on Information Systems, Milwaukee.

2. Ali, S. E. A., Lai, F.-W., Dominic, P. D. D., Brown, N., Lowry, P. B., & Ali, R. F. (2021). Stock market reactions to favorable and unfavorable information security events: A systematic literature review. *Computers & Security,* 110, 102451.

3. Ali, S. E. A., Lai, F.-W., & Hassan, R. (2020). Socio-economic factors on sector-wide systematic risk of information security breaches: Conceptual framework. 9th International Economics and Business Management Conference, Melaka, Malaysia.

4. Ali, S. E. A., Lai, F.-W., Hassan, R., & Shad, M. K. (2021). The long-run impact of information security breach announcements on investors' confidence: The context of efficient market hypothesis. *Sustainability*, 13 (3), 1066. https://doi.org/10.3390/su13031066

5. Aman, A., Naim, A. M., Isa, M. Y., & Ali, S. E. A. (2021). Factors affecting sukuk market development: empirical evidence from sukuk issuing economies. *International Journal of Islamic and Middle Eastern Finance and Management(Dec).* In Press. https://doi.org/10.1108/IMEFM-03-2020-0105

6. Arcuri, M., Brogi, M., & Gandolfi. (2017). How does cyber crime affect firms? The effect of information security breaches on stock returns. First Italian Conference on Cybersecurity, Venice, Italy.

7. Barber, B. M., & Lyon, J. D. (1997). Detecting long-run abnormal stock returns: The empirical power and specification of test statistics. *Journal of Financial Economics,* 43 (3), 341–372. https://doi.org/10.1016/S0304-405X(96)00890-2

8. Bissell, K., & Ponemon, L. (2019). The cost of cybercrime. Retrieved from https://www.accenture.com/us-en/insights/security/cost-cybercrime-study

9. Bose, I., & Leung, A. (2014). Do phishing alerts impact global corporations? A firm value analysis. *Decision Support Systems,* 64 (C), 67–78. https://doi.org/10.1016/j.dss.2014.04.006

10. Bose, I., & Leung, A. (2019). Adoption of identity theft countermeasures and its short and long-term impact on firm value. *MIS Quarterly,* 43 (1), 313–327. https://doi.org/10.25300/MISQ/2019/14192

11. Bouveret, A. (2018). *Cyber risk for the financial sector: A framework for quantitative assessment.* International Monetary Fund.

12. Chang, K.-C., Gao, Y.-K., & Lee, S.-C. (2020). The effect of data theft on a firm's short-term and long-term market value. *Mathematics*, 8 (5), 808. https://doi.org/10.3390/math8050808

13. Chen, X., Bose, I., Leung, A. C. M., & Guo, C. (2011). Assessing the severity of phishing attacks: A hybrid data mining approach. *Decision Support Systems*, 50 (4), 662–672.

14. Connelly, B., Certo, S. T., Ireland, R. D., & Reutzel, C. (2011). Signaling theory: A review and assessment. *Journal of Management,* 37 (1), 39–67.

15. Das, S., Mukhopadhyay, A., & Anand, M. (2012). Stock market response to information security breach: A study using firm and attack characteristics. *Journal of Information Privacy and Security,* 8 (4), 27–55.

16. De Groot, J. (2020). The history of data breaches. Digital Guardian. Retrieved from https://digitalguardian.com/blog/history-data-breaches

17. Du, J., Mickiewicz, T., & Douch, M. (2021). Individual and institutional ownership, firm age and productivity. *Journal of Competitiveness*, 13 (1), 23–41. https://doi.org/10.7441/joc.2021.01.02

18. Fama, E. (1970). Efficient capital markets: A review of theory and empirical work. *The Journal of Finance,* 25 (2), 383–417.

19. Fama, E. (1998). Market efficiency, long-term returns, and behavioral finance. *Journal of Financial Economics,* 49 (3), 283–306.

20. Fung, B. (2018). Equifax's massive 2017 data breach keeps getting worse. Retrieved from https://www.washingtonpost.com/news/the-switch/wp/2018/03/01/equifax-keeps-finding-millions-more-people-who-were-affected-by-its-massive-data-breach/?noredirect¼on&utm_term¼.36a8868c885d

21. Gatzlaff, K. M., & McCullough, K. A. (2010). The effect of data breaches on shareholder wealth. *Risk Management and Insurance Review*, 13 (1), 61–83.

22. Goel, S., & Shawky, H. A. (2009). Estimating the market impact of security breach announcements on firm values. *Information & Management*, 46 (7), 404–410. https://doi.org/10.1016/j.im.2009.06.005

23. Goode, S., Hoehle, H., Venkatesh, V., & Brown, S. A. (2017). User compensation as a data breach recovery action: An investigation of the Sony PlayStation network breach. *MIS Quarterly*, 41 (3), 703–727.

24. Gordon, L., Loeb, M., & Sohail, T. (2010). Market value of voluntary disclosures concerning information security. *MIS Quarterly,* 34 (3), 567–594. https://doi.org/10.2307/25750692

25. Hamad, S., Draz, M. U., & Lai, F.-W. (2020). The impact of corporate governance and sustainability reporting on integrated reporting: A conceptual framework. *Sage Open,* 10 (2), 1–15.

26. Helm, R., & Mark, A. (2007). Implications from cue utilisation theory and signalling theory for firm reputation and the marketing of new products. *International Journal of Product Development*, 4 (2), 396–411.

27. Hendricks, K. B., & Singhal, V. R. (2005). An empirical analysis of the effect of supply chain disruptions on long-run stock price performance and equity risk of the firm. *Production and Operations Management*, 14 (1), 35–52.

28. Hendricks, K. B., & Singhal, V. R. (2014). The effect of demand–supply mismatches on firm risk. *Production and Operations Management,* 23 (12), 2137–2151.

29. Hinz, O., Nofer, M., Schiereck, D., & Trillig, J. (2015). The influence of data theft on the share prices and systematic risk of consumer electronics companies. *Information & Management,* 52 (3), 337–347. https://doi.org/10.1016/j.im.2014.12.006

30. Hovav, A., Han, J. Y., & Kim, J. (2017). Market reaction to security breach announcements: Evidence from South Korea. *Data Base for Advances in Information Systems*, 48 (1), 11–52. https://doi.org/10.1145/3051473.3051476

31. Huang, Q., Zhang, H., Chen, J., & He, M. (2017). Quantile regression models and their applications: a review. *Journal of Biometrics & Biostatistics*, 8 (3), 354. https://doi.org/10.4172/2155-6180.1000354

32. Huang, Y. (2012). *Long-term abnormal stock performance: UK evidence.* (PhD). University of Exeter

33. IBM, & Ponemon. (2020). Cost of a data breach report. Retrieved from Michigan, USA: https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/

34. Kannan, K., Rees, J., & Sridhar, S. (2007). Market reactions to information security breach announcements: An empirical analysis. *International Journal of Electronic Commerce,* 12 (1), 69-91. https://doi.org/10.2753/JEC1086-4415120103

35. Kolodgy, C. (2021). Cybersecurity Fosters Competitive Advantage. Security Boulevard. Retrieved from https://securityboulevard.com/2021/05/cybersecurity-fosters-competitive-advantage/

36. Kothari, S., & Warner, J. B. (1997). Measuring long-horizon security price performance. *Journal of Financial Economics,* 43 (3), 301–339.

37. Lyon, J. D., Barber, B. M., & Tsai, C. L. (1999). Improved methods for tests of long-run abnormal stock returns. *The Journal of Finance*, 54 (1), 165–201. https://doi.org/10.1111/0022-1082.00101

38. Malhotra, A., & Malhotra, C. (2011). Evaluating customer information breaches as service failures: An event study approach. *Journal of Service Research*, 14 (1), 44–59.

39. McAfee. (2021). Hidden costs of cybercrime. Retrieved from https://www.csis.org/analysis/hidden-costs-cybercrime

40. Modi, S. B., Wiles, M. A., & Mishra, S. (2015). Shareholder value implications of service failures in triads: The case of customer information security breaches. *Journal of Operations Management,* 35, 21–39. https://doi.org/10.1016/j.jom.2014.10.003

41. Njenga, K., & Lowry, P. B. (2018). Information security policy violations: A grounded theory approach to counterfactual balance and tensions. Paper presented at the Dewald Roode Workshop in Information Systems Security, Cape Town.

42. Olcott, J. (2019). Cybersecurity Vs. Information Security: Is There A Difference? Retrieved from https://www.bitsight.com/blog/cybersecurity-vs-information-security

43. Özpolat, K., Gao, G., Jank, W., & Viswanathan, S. (2013). Research note—The value of third-party assurance seals in online retailing: An empirical investigation. *Information Systems Research,* 24 (4), 1100–1111. https://doi.org/10.1287/isre.2013.0489

44. Pavlou, P. A., Liang, H., & Xue, Y. (2007). Understanding and mitigating uncertainty in online exchange relationships: A principal-agent perspective. *MIS Quarterly,* 31 (1), 105-136. https://doi.org/10.2307/25148783

45. Pirounias, S., Mermigas, D., & Patsakis, C. (2014). The relation between information security events and firm market value, empirical evidence on recent disclosures: An extension of the GLZ study. *Journal of Information Security and Applications,* 19 (4-5), 257–271. https://doi.org/10.1016/j.jisa.2014.07.001

46. Raghu, T., Woo, W., Mohan, S., & Rao, H. R. (2008). Market reaction to patent infringement litigations in the information technology industry. *Information Systems Frontiers*, 10 (1), 61–75.

47. Ray, S., Ow, T., & Kim, S. S. (2011). Security assurance: How online service providers can influence security control perceptions and gain trust. *Decision Sciences*, 42 (2), 391–412.

48. Richardson, V. J., Smith, R. E., & Watson, M. W. (2019). Much ado about nothing: The (lack of) economic impact of data privacy breaches. *Journal of Information Systems*, 33 (3), 227–265. https://doi.org/10.2308/isys-52379

49. Rosati, P., Cummins, M., Deeney, P., Gogolin, F., van der Werff, L., & Lynn, T. (2017). The effect of data breach announcements beyond the stock price: Empirical evidence on market activity. *International Review of Financial Analysis,* 49 (1), 146–154. https://doi.org/10.1016/j.irfa.2017.01.001

50. Rosati, P., Deeney, P., Cummins, M., Van der Werff, L., & Lynn, T. (2019). Social media and stock price reaction to data breach announcements: Evidence from US listed companies. *Research in International Business Finance,* 47, 458–469. https://doi.org/10.1016/j.ribaf.2018.09.007

51. Rutta, M., & Diamond, C. J. (2018). SEC Fines Yahoo $35 Million for Failure to Timely Disclose a Cyber Breach. Retrieved from https://www.whitecase.com/publications/alert/sec-fines-yahoo-35-million-failure-timely-disclose-cyber-breach

52. Schatz, D., & Bashroush, R. (2016). The impact of repeated data breach events on organisations' market value. *Information & Computer Security,* 24 (1), 73–92. https://doi.org/10.1108/ICS-03-2014-0020

53. Sinanaj, G., & Muntermann, J. (2013). Assessing corporate reputational damage of data breaches: An empirical analysis. Paper presented at the 26th Bled EConference - EInnovations Challenges and Impacts for Individuals, Organizations and Society, Bled, Slovenia.

54. Smith, K. T., Jones, A., Johnson, L., & Smith, L. M. (2019). Examination of cybercrime and its effects on corporate stock value. *Journal of Information, Communication and Ethics in Society,* 17 (1), 42–60. https://doi.org/10.1108/jices-02-2018-0010

55. Spence, M. (1978). *Job market signaling. Uncertainty in Economics.* Amsterdam: Elsevier.

56. Spence, M. (2002). Signaling in retrospect and the informational structure of markets. *American Economic Review,* 92 (3), 434–459.

57. Telang, R., & Wattal, S. (2007). An empirical analysis of the impact of software vulnerability announcements on firm stock price. *IEEE Transactions on Software Engineering,* 33 (8), 544–557.

58. Tweneboah-Kodua, S., Atsu, F., & Buchanan, W. (2018). Impact of cyberattacks on stock performance: A comparative study. *Information and Computer Security*, 26 (5), 637–652. https://doi.org/10.1108/ICS-05-2018-0060

59. Tweneboah-Koduah, S., Atsu, F., & Prasad, R. (2020). Reaction of stock volatility to data breach: an event study. *Journal of Cyber Security and Mobility,* 9 (3), 355–384. https://doi.org/10.13052/jcsm2245-1439.931

60. Yayla, A. A., & Hu, Q. (2011). The impact of information security events on the stock value of firms: The effect of contingency factors. *Journal of Information Technology*, 26 (1), 60–77. https://doi.org/10.1057/jit.2010.4

Contact information

Syed Emad Azhar Ali, corresponding author
Universiti Teknologi PETRONAS,
Department of Management & Humanities,
Malaysia
E-mail: syed_17007896@utp.edu.my
ORCID: 0000-0003-3426-3223

Associate Professor Dr Fong-Woon Lai, PhD.
Universiti Teknologi PETRONAS,
Department of Management & Humanities,
Malaysia
E-mail: laifongwoon@utp.edu.my

Assistant Professor, Ameenullah Aman, PhD.
Business Administration Department,
Iqra University,
Pakistan
Email: ameenullahaman.s@gmail.com
ORCID: 0000-0001-9652-9686

Muhammad Furquan Saleem
Research Facilitation Unit,
Iqra University,
Pakistan
E-mail: furquan.saleem@yahoo.com
ORCID: 0000-0003-3299-732X

Salaheldin Hamad
Faculty of Commerce,
Kafrelsheikh University,
Egypt
Email: salah.hamad@com.kfs.edu.eg
ORCID: 0000-0002-9444-1493