Syed Emad Azhar Ali, Fong-Woon Lai, P. D. D. Dominic, *Nicholas James Brown, Paul Benjamin Lowry, and Rao Faizan Ali (2021). "Stock market reactions to favorable and unfavorable information security events: A systematic literature review" *Computers & Security* (C&S) (accepted 17-Aug-2021) (doi: https://doi.org/10.1016/j.cose.2021.102451).

If you have any questions, would like a copy of the final version of the article, or would like copies of other articles we've published, please contact any of us directly, as follows:

- **Syed Emad Azhar Ali**
  - Ph.D. student, Management from Universiti Teknologi PETRONAS, Malaysia
  - Website: https://scholar.google.com/citations?user=smByezoAAAAJ&hl=en&inst=13410158990364976897
- **Dr. Fong-Woon Lai**
  - Department Chair and Associate Professor at the Department of Management and Humanities, Universiti Teknologi PETRONAS, Malaysia
  - Email:
  - Website: https://scholar.google.com.my/citations?user=j0ZfHxIAAAAJ&hl=en&inst=13410158990364976897
- **Dr. Dhanapal Durai Dominic**
  - Associate Professor at Universiti Teknologi PETRONAS, Malaysia
  - Email: dhanapal_d@utp.edu.my
  - Website: https://scholar.google.com.my/citations?user=mKi4P7AAAAAJ&hl=en&inst=13410158990364976897
- ***Prof. Paul Benjamin Lowry,** Eminent Scholar and Suzanne Parker Thornhill Chair Professor
  - Business Information Technology, Pamplin College of Business
  - Virginia Tech
  - Email: Paul.Lowry.PhD@gmail.com
  - Website: https://sites.google.com/site/professorlowrypaulbenjamin/home
  - System to request Paul's articles: https://seanacademic.qualtrics.com/SE/?SID=SV_7WCaP0V7FA0GWWx
- **Nicholas James Brown**
  - Ph.D. student, Business Information Technology, Pamplin College of Business
  - Virginia Tech
  - Email: nichb15@vt.edu
  - Website: https://bit.vt.edu/faculty/directory/brown.html

- **Rao Faizan Ali**
    - Ph.D. student, Computer and Information Systems, Universiti Teknologi PETRONAS, Malaysia
    - Website: https://www.linkedin.com/in/rao-faizan-ali-68b69168/?originalSubdomain=my

*corresponding author

Stock Market Reactions to Favorable and Unfavorable Information Security Events: A Systematic Literature Review

ABSTRACT

The rapid digital transformations across every industry sector, accelerated partly due to the COVID-19 pandemic, have increased organizations' use of information systems for operational and strategic purposes. These organizational responses have led to a confluence of digital, biological, and physical technologies that are revolutionizing business practices and workflows. But accompanying the pervasive use of digital technologies and the evolutionary nature of digital assets, is a shifting world of cyberattacks and information security (ISec) cybercrimes. Dynamic cybercrimes make it increasingly difficult for managers and researchers to anticipate the types, magnitude, and severity of future information security (ISec) breaches. Thus, we perform a systematic literature review (SLR) that explores, gathers, and categorizes *event studies* to examine the influence of favorable and unfavorable ISec events on stock markets. We extend the research conducted by Spanos and Angelis (2016) and provide a comprehensive understanding of the market's efficiency to process public information released about ISec events, ISec contingency factors, and the influence of ISec events on stock prices and factors other than price. Our systematic search reveals 58 relevant papers that include 80 studies. We find that in 75% of the studies ISec events can significantly affect a company's stock market performance, and that such effects are primarily exhibited within two days before and after the event day. Further, the magnitude of abnormal returns is higher in studies examining unfavorable ISec events, such as ISec breaches, compared to abnormal returns from favorable events, such as ISec investments and ISec certifications. In the end, our SLR serves as a foundation for ISec and management communities to build upon to keep industry and academia apprised of continually developing trends, new attack vectors and types of data breaches, protective ISec behaviors and programs, and their subsequent influences on stock market values and returns.

Keywords: Event study methodology (ESM), information security (ISec) breaches, systematic literature review (SLR), ISec events, ISec investments, efficient market hypothesis, contingency factors, abnormal returns.

1. Introduction

The proliferation of information technology has had a profound effect on every sector of the economy. As the fourth industrial revolution (IR4.0), Internet of Things (IoT), and cloud infrastructure become more prevalent, a rising number of businesses leverage information systems to improve the efficiency of their internal and external operations. But systems that can produce impressive advantages also pose a risk to information security (ISec), because such information can be illegally accessed, distributed, manipulated, altered, or destroyed by hostile or unauthorized parties. The World Economic Forum on global risk perception describes the risk of an ISec breach as the most concerning and likeliest risk after natural disasters (Collins 2018, 2019). Unfortunately, in today's business climate, the prevailing presumption of an ISec breach has become the new norm (Hayden 2013; Njenga and Lowry 2018), where breaches are expanding in size and consequence (De Groot 2019).

Given its negative consequences when poorly governed, ISec is a primary concern for both executives and accounting professionals (AICPA 2015; Protiviti 2016). Stakeholders also demand ISec measures that are robust against breaches—such as spyware, malware, denial-of-service attacks, phishing, ransomware, and other threats (Jansen et al. 2013; Lukonga 2018; Smith et al. 2011). Consequently, multinational ISec regulations, corporate ISec governance and strategies, and advanced operational defenses have been established and continually updated to counter the growing risks of ISec breaches (Gordon et al. 2010; Hina et al. 2019; Kwon and Johnson 2015; Lowry et al. 2017; Shin and Lowry 2020; Wagner et al. 2019). However, research that provides a comprehensive understanding of the market's efficiency to process the economic consequences of ISec breaches or protective ISec activities is limited.

To date, numerous event studies have examined the effects of ISec events on company stock performance, and these studies have involved various research contexts, dimensions, and results. However, researchers have not identified which research contexts and event study dimensions are most impactful—partly because the research contexts and dimensions have evolved as technologies have advanced, thereby leading to variations in the types of ISec events that can occur. Further, researchers have exhibited different motivations for investigating ISec events and have used various theoretical lenses to inspect these

phenomena. This can lead to disjointed efforts in advancing ISec research. As ISec research on company stock performance grows, reviewing such research is vital to understanding how the research discourse has evolved.

Consequently, our objective is to perform a systematic literature review (SLR) that searches for, gathers, categorizes, and reviews articles that have addressed stock market reactions to ISec-event announcements, primarily with a specific interest to extend the research conducted by Spanos and Angelis (2016). ISec events can have a *contagion effect* in which they not just affect a target firm but can also affect the stock returns of competitors and other associated firms (Jeong et al. 2019; Pelletier 2017; Rosati et al. 2017). Although most studies have examined the influence of ISec events on stock price, few have examined their influence on company performance measures other than price. Therefore, to provide a new lens to view and approach future ISec-event studies, our review describes the effects of various ISec contingency factors on company performance measures beyond those of stock price.

First, practitioners commonly define an *ISec breach* as an event in which an unauthorized person has possibly looked at, stolen, or used sensitive, safe, or confidential information (Adebayo 2012; Imran et al. 2018). The firm experiencing the breach must deal with losses (e.g., loss of reputation and trust leading to lost business in the future) and various forms of litigation. Illegal access to passwords, destruction, and manipulation of data, the shutdown of computer facilities, and modification and theft of computer software are examples of ISec breaches and violations. These types of ISec breaches suffered by firms are considered *unfavorable ISec events*.

Second, firms have an incentive to announce protective ISec measures to provide security assurances to their stakeholders (Lowry et al. 2011). As a result, firms make frequent capital investments to avoid ISec breaches (Chai et al. 2011; Jeong et al. 2019) and they continually assess and enhance their ISec policies—for example, by introducing identity theft countermeasures, dynamic password generators, SMS-based one-time passwords, personal digital certifications, and electronic signatures (Bose and Leung 2013; Bose and Leung 2019). Important for our review, such measures taken to enhance ISec protocols are considered *favorable ISec events*.

Third, ISec events, whether favorable or unfavorable, can influence a firm's financial results tangibly and intangibly (Bose and Leung 2014; Bose and Leung 2019; Cavusoglu et al. 2004). *Tangible effects* encompass direct changes in revenues or market capitalization occurring over the long run. By contrast, *intangible effects* include changes in the trust and confidence of business stakeholders, especially shareholders who invest in firms publicly listed on stock exchanges, such as the NASDAQ and the New York Stock Exchange (NYSE). However, it is challenging to measure the influence of an ISec event on a company's stock performance.[i] Researchers have attempted to measure the effects on a company's stock performance by using the *event study methodology* (ESM) (MacKinlay 1997). An underlying assumption of this method is the *efficient market hypothesis* (EMH) in its semistrong form (Schwartz 1970), which is described as the efficiency of markets to quickly process information (Fama 1991) where stock prices adjust rapidly to newly released public data. Therefore, according to the EMH, the share price of a firm should incorporate all the available information concerning that firm. Thus, the effects of a publicly disclosed ISec event should be reflected in a company's stock price.

Based on this general assumption of the EMH, researchers have examined the influence of both types of ISec events—favorable and unfavorable—on the stock market. Regarding unfavorable events, researchers have studied the effects of denial-of-service attacks, privacy breaches, phishing, software vulnerabilities, Heartbleed bugs, and website defacement. These studies examined the consequences of such events on the stock performances of breached firms (Campbell et al. 2003; Cavusoglu et al. 2004; Ettredge and Richardson 2002; Garg et al. 2003; Hovav and D'Arcy 2004; Hovav and D'Arcy 2005), ISec firms (Cavusoglu et al. 2004; Ettredge and Richardson 2002), and competitors of breached firms (Hinz et al. 2015; Jeong et al. 2019; Kim 2013). Similarly, favorable ISec events such as technical and nontechnical ISec investments, ISec certifications, and ISec legislation have been studied to determine their influences on company stock performance (Bose and Leung 2013; Chai et al. 2011; Jeong et al. 2019; Khansa et al. 2012).

The literature has indicated that unfavorable ISec events significantly and negatively influence the stock price of the concerned firm and can thus decrease investor confidence. Extant literature has also focused on

other dimensions of ISec events and stock market performance measures such as the EMH for ISec events, ISec contingency factors, and factors beyond stock price. Review studies have provided a valuable synthesis of research on the financial outcomes of ISec events; however, further examination is required to understand the efficiency of markets to process the contingency effects related to ISec events. We noticed that extant review studies have neglected to examine these contingency factors. Moreover, the assessment is driven by the need to evaluate the EMH for ISec events, major ISec contingency factors, and stock market factors other than price. Our research questions (RQs) related to the current SLR are therefore as follows:

> **RQ1**: What are the major study characteristics and results of studies investigating the effects of ISec events on company stock performance?
>
> **RQ2**: Which levels of stock market efficiency are seen in the literature as related to ISec events?
>
> **RQ3**: What are the most important ISec contingency factors examined in the research literature?
>
> **RQ4**: Aside from the effects on a company's stock price, what ISec-event outcomes have been examined in this research discourse?

Our SLC explores online sources of interrelated studies and filters the studies relevant to our research questions. A key objective of our SLR is to evaluate the efficiency of stock markets related to ISec events and contingency factors. we thus review the influence of ISec events on market reactions, extract overall conclusions, and detail research opportunities and policy implications for researchers and managers.

2. Related Research and Background

Our SLR focuses on research examining the intersection of ISec events and affected companies' stock market performance. We namely focus on determining (1) market efficiency for ISec events, (2) ISec contingency factors, and (3) factors beyond stock price. First, we present a brief review on the findings from seminal SLRs and the discoveries noted by these teams of researchers. Next, we provide background information on event studies and the EMH. Last, we describe types of ISec events and the effects of publicly announcing these events on companies' stock prices and other factors.

2.1. Related Research from Extant SLRs

Our SLR falls under the umbrella of reviews on information technology (IT) events and their influence on

stock markets. Namely, extant studies examine either the influence of IT investments (e.g., ecommerce, information systems, DSS, ERP, CRM) or overall IT events (together with ISec, IT investments, IT subcontracting) on stock markets. Three ESM SLRs investigate the effects of IT investments on the stock market (Dehning et al. 2003; Roztocki and Weistroffer 2009b; Zhang and Huang 2009). Another set of three ESM SLRs consider the effects of various IT events, including some ISec-related events, on stock markets (Roztocki and Weistroffer 2011; Roztocki and Weistroffer 2008, 2009a). Nevertheless, most of the IT events these three studies consider are not ISec-related events. Similarly, a later SLR with a similar focus on IT events includes only nine articles related to ISec events (Konchitchki and O'Leary 2011), and another review of 209 articles focuses on ISec risks—but only four of the articles assess the influence of ISec events on stock markets (Eling and Schnell 2016). Finally, Spanos and Angelis (2016) conduct the most relevant SLR of event studies, where they review 37 articles and initiate the call to action to ISec researchers to investigate the effects of ISec-related incidents on companies' stock prices. They discover that 75.6% of the studies show a statistically significant influence between an ISec event and a company's stock price.

2.2. ESM and EMH

Studies analyze stock market efficiency for ISec events by scrutinizing the near-immediate or delayed market reactions to ISec-event announcements. Studies also examine the consequences of corporate events (e.g., mergers, acquisitions, CEO replacements) on stock markets under three forms of the EMH: strong, semistrong, and weak (Malkiel and Fama 1970). The *strong form* of market efficiency occurs when stock market reactions concerning an event are proactive and instantaneous on the event day ($t = 0$) or in some cases before the event day ($t = -1$, $t = -2$) (Fama 1991; Malkiel and Fama 1970). Accordingly, when information concerning a firm's ISec event is announced, an instantaneous or delayed adjustment in the stock price and returns of the firm in question may occur. The ESM is used to gauge the efficiency of markets by analyzing the cumulative abnormal returns (CARs) around the event day.

By contrast, the *semistrong form* of the EMH reflects conditions in which the effects of ISec-event announcements will be witnessed only when such an event is announced (i.e., $t = 0$, $t = +1$, $t = +2$) (Hinz et al. 2015; Masaki Ishiguro 2006; Sinanaj and Muntermann 2013). Studies find that the effects of ISec-

event announcements can be seen in the stock market before the event day (i.e., *t = -1, t = -2*) (Arcuri et al. 2017; Khansa et al. 2012; Liginlal et al. 2009). Finally, the *weak form* of the EMH reflects an absence of correlation between historical prices and future price performance, such that all public information is fully reflected in stock prices and future trends cannot be projected by studying past pricing actions and events (i.e., random walk theory[ii]) (Malkiel and Fama 1970).

To assess the EMH, researchers use the ESM. The efficiency level will be stronger if the news of an "ISec event" triggers an instantaneous and significant change in stock price and returns of the concerned firm (i.e., within one or two days around the "event day") (MacKinlay 1997; Malkiel and Fama 1970). Although most event studies find that an ISec event will have a substantial negative influence on stock price and will create major CARs, scholars have not yet developed a consensus regarding the level of market efficiency for ISec events. Researchers conclude that the major CARs triggered by an ISec event could be seen on the event day and within two days of the event, which demonstrates a semistrong form of efficiency (Chen et al. 2011; Garg et al. 2003; Hovav and D'Arcy 2003; Shiller 2000). Other studies illustrate the presence of major CARs seven days after an ISec event (Hovav et al. 2017; Masaki Ishiguro 2006; Rosati et al. 2019; Yayla and Hu 2011). Still, more studies show the presence of CARs before the announcement of an ISec event (Goel and Shawky 2009; Janze 2017; Liginlal et al. 2009). Furthermore, market efficiency levels for favorable and unfavorable ISec events might differ. Therefore, an SLR examining market efficiency can provide ISec researchers with pragmatic time frames for setting estimation and event windows to conduct future event studies on CARs.

2.3. Types of ISec Events

A considerable body of research explores various issues related to ISec risk management, such as ISec investments, institutional influence on innovation and ISec policies (Hsu et al. 2012), ISec climate and ISec policy compliance (Dong et al. 2021). Another line of research focuses on market consequences of ISec-related disclosures (Gordon et al. 2010; Wang et al. 2013) and ISec breach announcements (Cao et al. 2010; Cavusoglu et al. 2004; Goel and Shawky 2009; Goldstein et al. 2011; Gordon et al. 2010; Hinz et al. 2015; Kannan et al. 2007; Wang et al. 2013) using the ESM. We categorize these ISec-event studies as addressing

either favorable or unfavorable ISec-event announcements, and this categorization aligns with approaches found in IS journals and conferences. Both event types will have a short-term and long-term financial effect on the firm's financials. In unfavorable ISec events, the short-term costs relate primarily to investigation and remedial operations, legal advice services, and fines. Long-term costs are attributable to loss of current and potential sales and a weakening of customer or partner confidence (Almadhoun et al. 2011; Cavusoglu et al. 2004). For favorable ISec events, the financial gain might reflect over different time horizons (Bose and Leung 2019; Deane et al. 2019).

Irrespective of the type of ISec event, the subsequent financial outcomes can be tangible or intangible. It is possible to estimate abnormality for tangible effects such as sales, material, labor, and insurance. However, it is challenging to estimate abnormality related to intangible effects, such as trust and investor confidence. Intangible effects are essential in assessing the financial consequences of an ISec event on a firm. These effects have widespread influences on a company's potential cash flow and on investor confidence. Any abnormality in investor confidence can influence the firm's insurance costs and its ability to raise capital in debt and equity markets.

2.4. Role of ISec Contingency Factors

In addition to the market efficiency for ISec events, it is pertinent to identify the cross-sectional factors associated with an ISec event. *ISec contingency factors* explain the magnitude of significant CARs after an ISec event (Yayla and Hu 2011). These are the characteristics specific to an ISec event, affected firm, or industry. They can help investors and managers assess the level of sensitivity in stock returns linked with an ISec event. For example, studies find that ISec-breach type and the type of information compromised are factors influencing the magnitude of substantial CARs (Garg et al. 2003; Gordon et al. 2010; Janze 2017; Jeong et al. 2019; Yayla and Hu 2011). Other studies incorporate firm-specific factors—such as a firm's size, growth, credit ratings, ownership status (owned or subsidiary), and IT intensity—as functions of CARs after an ISec event (Garg et al. 2003; Gordon et al. 2010; Janze 2017; Yayla and Hu 2011). By contrast, other studies find that CARs after an ISec event are specific to industry type (i.e., IT intensity differs among industries) (Broadbent et al. 1999; Dardan and Dardan 2005; Im et al. 2001; Santos et al.

1993). Ultimately, the effects on CARs will depend on the use of IT in that specific industry (Bose and Leung 2014; Cavusoglu et al. 2004; Im et al. 2001; Morse et al. 2011; Tweneboah-Kodua et al. 2018; Yayla and Hu 2011).

The factors associated with an ISec event that can influence the magnitude of substantial CARs include ISec-breach or -attack characteristics (Arcuri et al. 2017; Bose and Leung 2014; Hovav and D'Arcy 2004), the type of ISec measure or investment announced by a firm (Deane et al. 2019; Khansa et al. 2012), firm characteristics (Cavusoglu et al. 2004; Goel and Shawky 2009; Rosati et al. 2017), and industry characteristics (Pirounias et al. 2014; Yayla and Hu 2011). According to Yayla and Hu (2011), these factors are collectively termed "information security contingency factors" (see **Fig. 1**). However, researchers have not conducted an SLR that presents a comprehensive analysis of all contingency-factor types and their effects on market reactions or that explains the magnitude of CARs. Thus, the comprehensive analysis in our SLR will help ISec researchers focus on the contingency factors that have the most significant influence on stock market reactions after an ISec event.

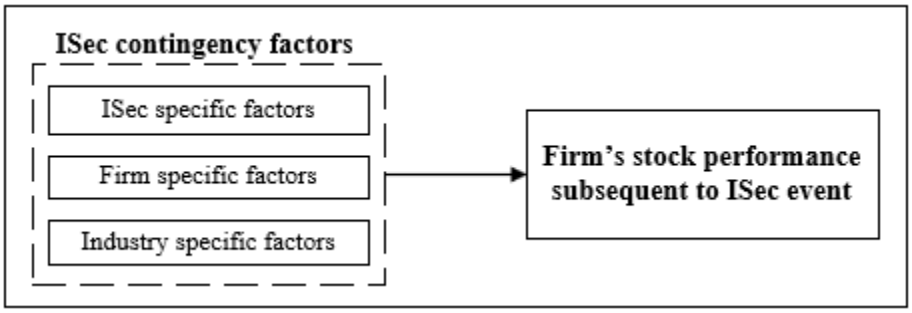

Fig 1. ISec contingency factors as drivers of stock performance after an ISec event.

2.5. Stock Price as a Proxy for Financial Consequence of ISec Events

Given that the estimation of financial consequences involves a broad range of elements spanning various periods, the estimation of CARs is difficult. The price adjustment following the declaration of a data breach is often embraced as an indicator. This supposition builds on the semistrong EMH as derived from Malkiel and Fama (1970). According to this assumption, the stock price contains all public knowledge and all potential anticipated cash flows to and from a firm. Based on this hypothesis, studies examine the economic effects of an ISec event using the stock price of a concerned firm as a proxy.

From the investor's point of view, examining the stock price behavior as a proxy of investor confidence is essential because stock prices reflect current and expected future costs and risks associated with a particular ISec event (Shiller 2000). It is also crucial to the affected firm's management teams because stock prices reflect the firm's market value, which indicates the overall strength and health of a company. The factors critical to determining a firm's future cost of capital—credit ratings, employee and manager compensation, the management team's firing decisions—are inherent in the market valuation of a company.

3. Methodology

We performed an SLR to select and code relevant articles to sufficiently answer our RQs. This is a replicable, straightforward, objective, impartial, and comprehensive methodology (Boell and Cecez-Kecmanovic 2015). We followed the SLR guidelines developed by Boell and Cecez-Kecmanovic (2015), because the guidelines are general and applicable to any literature review and have been applied in other ISec reviews (Boell and Cecez-Kecmanovic 2015; Eling and Schnell 2016). Our SLR includes the same sequence, which involves three stages: (1) the planning stage, (2) the conducting stage, and (3) the reporting stage. The steps of all three stages are shown in **Fig. 2**.

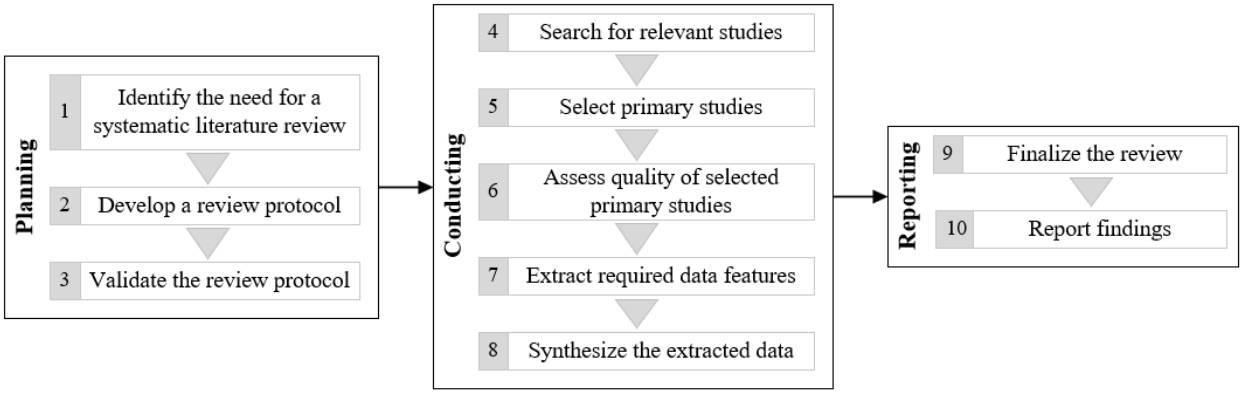

Fig. 2: Stages of our SLR.

3.1. Planning Stage

The "planning stage" begins with identifying the need for an SLR and developing a review protocol. Many previous studies examined market reactions to ISec events that involved distinct ISec characteristics, such as firm size, time frame, and industry type; however, researchers were not aware of whether market reactions to ISec events changed over time and which ISec characteristics led to these changes in reaction.

Namely, there is a lack of understanding of the stock market efficiency for ISec events, ISec contingency factors, and factors beyond a company's stock price.

In the second step of planning, we developed the review protocols. Essentially, the developed protocols characterize the overall "conducting stage" by identifying the activities necessary to proceed with the conducting stage (Eling and Schnell 2016; Kitchenham 2004; Yun et al. 2019). The activities identified were benchmarked and are detailed as follows:

- Defining the RQs
- Selecting the search strategy
- Explaining the study's inclusion/exclusion benchmarks
- Assessing the quality benchmark
- Selecting the data features to be extracted from the filtered papers

Subsequently, the review protocols were refined throughout the current SLR process. The refining of RQs is vital because the effective accomplishment of a review is dependent on the answers to these research questions (Khan et al. 2003).

To perform the search exhaustively, we used a combination of broad, automated searches using digital libraries and indexing systems and backward snowball techniques (Bezerra et al. 2014; Khan et al. 2003; Spanos and Angelis 2016). Under broad, automated searches, we first leveraged four well-known digital libraries, following the guidelines provided by Lowry (2018): (1) *ScienceDirect*® by Elsevier B.V., (2) IEEE *Xplore*® Digital Library by IEEE, (3) *Web of Science*™ by Clarivate, and (4) *Scopus*® by Elsevier B.V. Next, we used three additional specialized search engines to ensure the search was exhaustive: (1) Google Scholar® by Google, (2) Yahoo!™, and (3) RefSeek™ (privately held). In line with the subject matter of this review (i.e., the influence of ISec events on the stock market), search terms were determined. By using a sophisticated search string and joining Boolean operators, we formed three tiers of search terms. The first two tiers were based on the key terms related to the theme of this review (i.e., "information security" and "stock market"). The third tier was added to the search string with the term "event study." Accordingly, the collective search string we used is as follows:

```
((“Information Security” OR “Computer Security” OR “Network Security” OR
“Internet Security” OR “Information System Security” OR “Web Security” OR
“Software Security” OR “Application Security” OR “Cyber Security” OR “Data
```

Privacy" OR "Security") AND ("Market Value" OR "Stock Value" OR "Stock Market" OR "Stock Price" OR "Market Price" OR "Shareholder Wealth" OR "Firm Value" OR "Market Impact" OR "Share Price" OR "Shareholder Value" OR "Market Reactions" OR "Capital Market" OR "Market Securities") AND ("Event Study"))).

To reduce the number of unrelated papers retrieved in our search results, all searches were based entirely on research titles, keywords, and article abstracts. The backward snowball technique was used as a complement to the broad, automated search to hunt for papers not located by the first approach (Bezerra et al. 2014). This approach requires an iterative analysis of the references. Formally, we located new papers and compiled a collection of papers until we observed a degree of saturation in the references we reviewed.

The *inclusion/exclusion selection benchmark* was set up in line with the theme of this SLR: using the ESM to determine the influence of ISec events on a company's stock performance. The extracted articles were thus subjected to rigorous inclusion criteria. Specifically, the articles had to reference at least one study that used the ESM to examine stock market reactions to a firm's ISec event announcement. We reviewed the methods in each paper and did not use papers that claimed to be event studies but used other methods, such as content analysis, regression analysis, matching portfolio, or one-to-one matched sampling (Ali et al. 2021b; Chang et al. 2020). Importantly, because we analyzed event studies examining the effects of ISec events on the stock performance of a company, we excluded event studies that examined effects on other performance indicators (e.g., Sinanaj and Muntermann 2013; Zafar et al. 2012; Zafar et al. 2016). Moreover, the articles must have been published in the English language (Boell and Cecez-Kecmanovic 2015) and published online before January 1, 2020. We also excluded articles that included stock market reactions to general IT events not specific to a security-related event at a firm. Finally, we eliminated articles that did not report findings and articles that were not peer-reviewed (i.e., technical reports, working papers, project deliverables, and Ph.D. theses) (Petticrew and Roberts 2008).

We also examined *quality assessment* as another crucial factor, along with the inclusion/exclusion benchmark, to ensure that the articles included in our review met an acceptable and adequate quality level (Al-Emran et al. 2018). Thus, a study should at least partially meet the quality assessment benchmark to be included in the present SLR (Al-Emran et al. 2018; Shahzad et al. 2019; Yun et al. 2019). Based on this

benchmark, we reviewed every study to ensure each contained sufficiently clear and complete research objectives, descriptions of the data, methodological details, analysis procedures, and results given according to expected scientific standards.

The *selection of data features* to be extracted from the articles/papers was the last step in the review protocol development. This step ultimately helped us to answer our RQs (Kitchenham and Charters 2007). **Table 1** lists the features extracted from studies that correspond with the respective RQs:

Table 1. Items extracted for each research question.

For RQ#		Items extracted
1	(a)	Authors, year of publication, type of paper, name of journal/conference, type of event examined.
	(b)	Location of ISec events, estimation and event windows used, event sample size, estimation model, and the parametric and nonparametric tests used.
	(c)	Results of each study and the magnitude of significant CARs.
2		Extraction of significant event windows for an in-depth analysis of the EMH.
3		Extraction of significant and insignificant contingency factors.
4		Extraction of examined factors other than price on the influence of ISec events.

Notably, the RQs are directed toward those scholarly works that engaged the *ESM* to scrutinize the effect of an ISec event on company stock market performance. Thus, it is essential to explain the extracted items briefly and why each item is relevant for researchers. An adequate understanding of such items is necessary to interpret the emergent results, as presented in the next section. **Fig. 3** depicts the critical steps for conducting an ESM study (MacKinlay 1997), which we followed: (1) event identification, (2) justifying the length of the event window, (3) event sample size, (4) estimation model, and (5) testing the significance of CARs. Next, we briefly elucidate the significance of each step when conducting event studies.

(1) Event identification: The announcement of an event by a firm can provide researchers with opportunities to study events of interest. In line with the theme of this SLR, researchers identify the events of ISec breach announcements by firms and examine their influence on company stock performance. Moreover, the location of ISec events indicates the context (country) under which a phenomenon is applicable in an ESM study, and a higher number of event studies in the same context (country) signal a

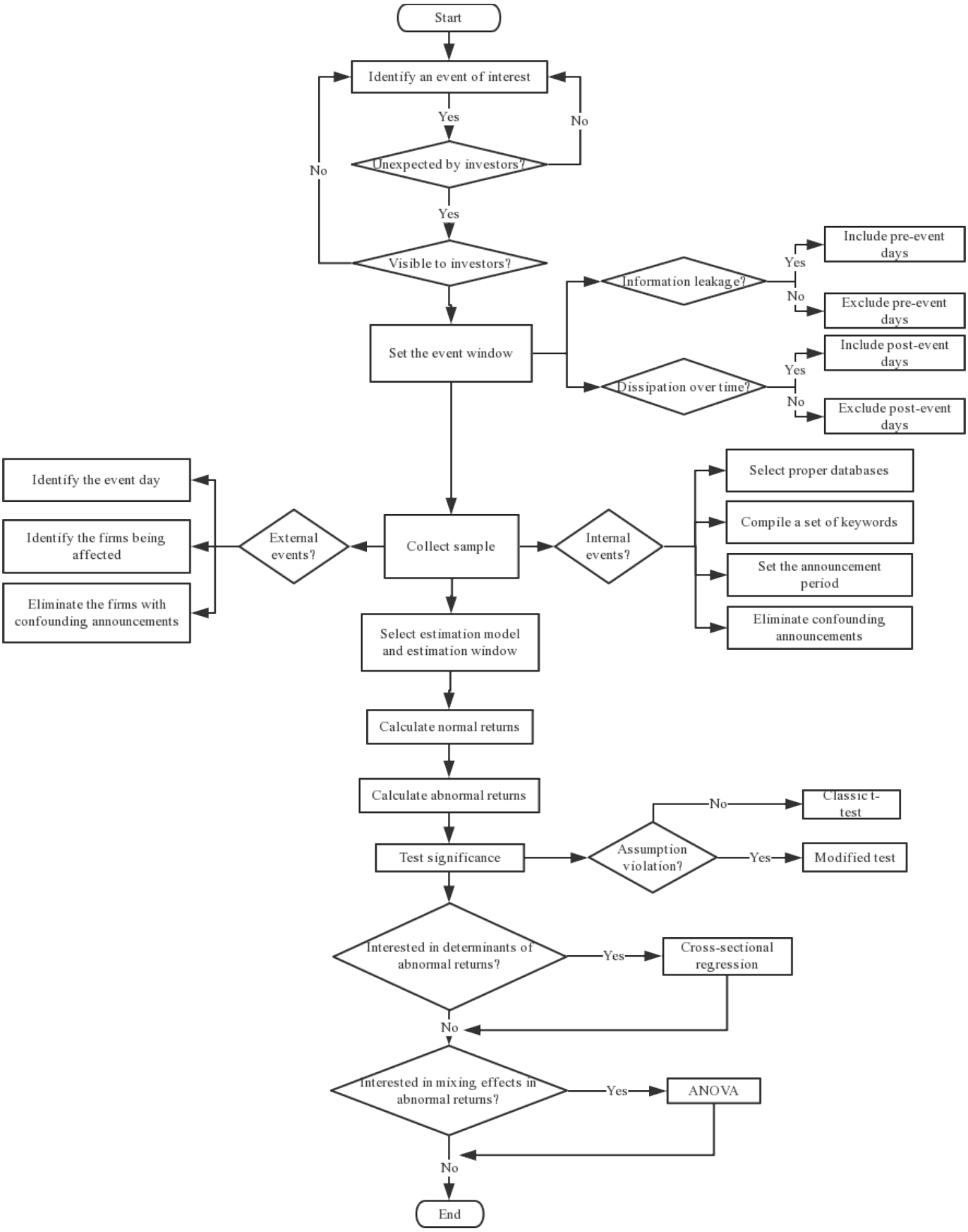

Fig. 3: Steps involved in conducting an ESM study.

stricter obligation by regulators in the country to announce events that are sensitive to investors in the stock market. **Table A2** (in Online Appendix A) presents the different types of ISec events along with the location of these events. Another crucial factor is whether the event is unpredictable before it is disclosed to investors and visible to investors when it is disclosed. This is because the EMH conviction that any company's news announcement will automatically reflect in its stock price (MacKinlay 1997; Malkiel and Fama 1970). If ISec event details are leaked, the stock price could be affected before the official announcement. Consequently, the market reaction on the day of the event may only be a residual adjustment of real expectations.

(2) Justifying the event window: The first stage of operationalizing an event study requires the researcher to set up and justify an event window over which an event's effect is to be tested. An event window is symbolized as (-x, +y). The date of an announcement is normally fixed at day 0. The event window (-x, +y) involves *x* trading days before day 0 to catch any information leaks and *y* trading days after day 0 to account for any delay in interpreting the information. The event window is usually extended for several days around the day of the event. Most studies use a shorter event analysis, from a day before the event to a few days after it. However, if theoretical explanations for information leaks or dissipation are found over a relatively long period, the event window may be extended (MacKinlay 1997). The use of alternate event windows as a robustness test is also a common approach in practice. As **Table A3** shows, several studies (Arcuri et al. 2014; Arcuri et al. 2017; Hovav and D'Arcy 2003; Hovav et al. 2017; Khansa and Liginlal 2011) used various event windows to assess the sensitivity of their results.

(3) Event sample size: A challenge for ESM scholars is to gather a sufficient event sample size to perform a robust statistical analysis. This is an arduous task that requires selecting applicable press releases that are known to have influenced investors' trading activities. **Table A3** exhibits the primary data sources used by studies to examine the effect of ISec events on the stock market. The second phase involves selecting search terms and timelines, which should be conservative to certify that the description of the event is clear and stable over time. The time ranges differ depending on the types of events and are a function of the frequency of events disclosed by publicly listed firms (i.e., in the current context, ISec

events). The last phase of finalizing the event sample size requires the elimination of confounding events. If these confounding events are not eliminated, they can unduly influence the calculation of CARs and thus weaken the internal validity.

(4) Estimation model: The next step requires selecting an appropriate model for estimating the CARs. Because only actual stock returns can be observed after the event, stock returns can be calculated only in the absence of the event. In an SLR grounded on ESM, but based on supply chain events, Ding et al. (2018) conclude that market model is employed in almost 90% of the studies. Meanwhile, few studies adopt the mean adjusted model, market-adjusted model, and Fama-French factor model. These estimation models suppose that stock returns are normal and distributed over time independently and identically. According to MacKinlay (1997), these suppositions are convincing, empirically true, and references to deviations from the suppositions are robust. Therefore, for estimation, ordinary least square regression is often used.

Once the estimation model is selected, the parameters in the factor models are calculated over the specified estimate window. In the literature, the estimation windows, as shown in **Table A3**, range from 1 day before the event to 300 days before the event. To overcome the bias in CARs caused by out-of-sample estimating, the estimation windows are typically extended, and the prediction windows are usually set to avoid overlap with the event window.

(5) Testing the significance of CARs: Cumulative outcomes from (2), (3), and (4) above help us to investigate the key study characteristics in RQ1. We then summarized findings from each study and analyzed the ARs using parametric and nonparametric statistical tests. Researchers have analyzed the ARs and their significance by measuring the real ex-post return of a company minus its estimated normal return over the event window. For firm i and event day t, the AR is

$$AR_{i,} = R_{i,} - \mathrm{E}\,(R_{i,t}), \qquad \text{eq. (1)}$$

Finally, the ARs are then aggregated across the number of days in an event window to compute the CAR for that specific event window. **Table A4** depicts the significant CARs and their magnitude in each study.

Last, statistical testing is necessary to calculate the significance of CARs. Studies include various parametric and nonparametric tests to check the significance of the obtained CARs. The *parametric t-test*

is the standard approach used in many event studies to measure the significance of cumulative CARs. Although this approach is based on CAR's independence and homoscedasticity assumptions, these assumptions can be violated in cases where event days are clustered and event-induced volatility is present. Thus, scholars also execute *nonparametric tests*, such as the Wilcoxon signed-rank test, Corrado's rank *t*-test, binomial sign test, and sign-*z* test, to report skewness in the distribution of the CARs. Nonparametric tests are an effective tool for controlling the nonnormal distribution and cross-sectional dependence in event studies. Consequently, parametric, and nonparametric tests are expected to exhibit appropriate tolerance levels ISec researchers measure to address skewness and cross-sectional dependence issues.

3.2. Conducting Stage

After we developed and validated the review protocols, we conducted our literature search (i.e., the conducting stage). **Fig. 4** illustrates the steps taken to derive the final number of papers selected for this review. We found 645 papers in the initial search process. After reading selected titles and abstracts to find unrelated papers or duplicates, we removed 530 papers, leaving 115. Afterward, using the inclusion/exclusion benchmark, we further removed 63 papers. This process yielded 52 papers from our broad, automated search. We later applied the backward snowball technique by searching through the references cited in other SLRs. After assessing the applicability of those references to our study, we ultimately included six more papers. In summary, our rigorous selection process and assessment of quality criteria yielded 58 papers.

Our appendix summarizes the excluded articles possibly relevant to the subject matter of our review but were scoped out for failing to meet our inclusion criteria (**Table A1** in Online Appendix A). Importantly, most articles were scoped out because they did not use the ESM, which is the predominant method used by scholars to examine the effects of unanticipated events such as data breaches on company stock performance. As a result, the current review includes an in-depth analysis of only the event studies that examined the influence of ISec events on a company's stock performance. Of the 12 excluded articles, seven did not use the ESM and thus did not align with our RQs. Two articles were scoped out because they were written in Korean, and their English versions were unavailable. One article referenced voluntary

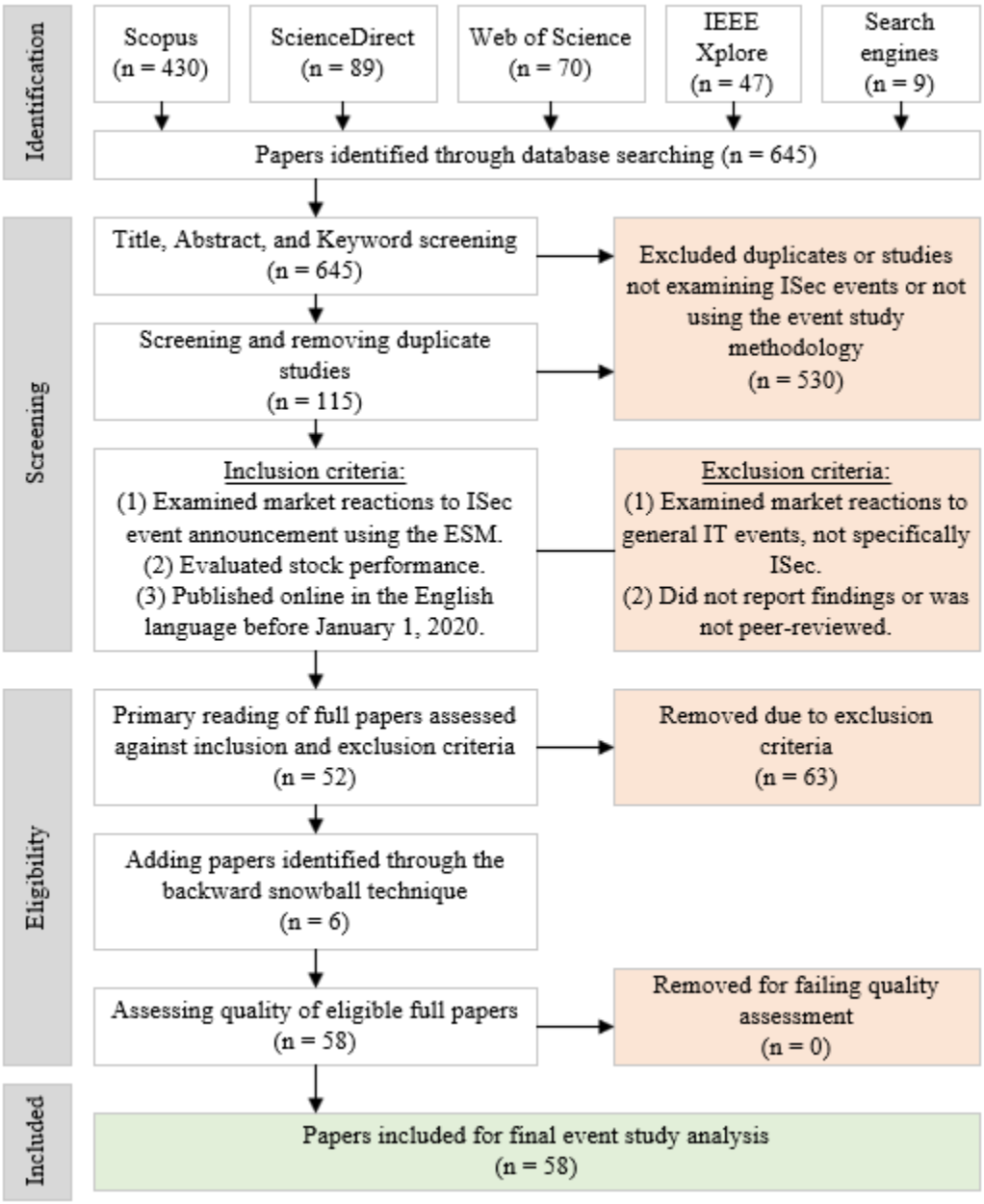

Fig 4. Steps to reach the number of reviewed papers.

disclosures by firms during 10-K filing at the end of the year, and another article was a working paper not indexed in a digital library. Finally, one article was excluded because it contained no empirical examination. The SLR results are reported in the next section as the third stage of SLR methodology.

4. Results of SLR

Here, we report the results of our SLR in relation to each of the four RQs (i.e., *reporting stage*). We first discuss the major study characteristics and features to answer RQ1. In the second section, we discuss our

findings on the levels of stock market efficiency for ISec events, thus answering RQ2. To answer RQ3, in the third section, we discuss the significance of various ISec contingency factors and their effects on company stock performance. In the fourth section, we answer RQ4 by discussing the effects ISec events have on factors other than a company's stock price.

4.1. Major Study Characteristics and Findings

The first research question (RQ1) of this review (i.e., to highlight the major study characteristics and results of each study), is quite broad, so we further segmented this exploration as follows: **(a)** publication credentials of the studies (Section 4.1.1.), **(b)** major dimensions employed by the studies (Section 4.1.2.), and **(c)** the summary results of these studies in terms of stock performance (Section 4.1.3.). **Table A2** summarizes the publication credentials of the 58 published papers included in this review. The features extracted from these studies include the author's name, year of publication, type of paper, name of the publication source, and type of ISec event examined. The major dimensions of the studies are presented in **Table A3** and partially in **Table A4. Table A3** summarizes the key ESM dimensions, including time interval, data source, estimation model, location of ISec events, estimation and event windows, and types of statistical tests. **Table A4** separately summarizes the major study dimension, event sample size.

4.1.1. Publication credentials

Table A2 identifies Bose & Leung and Hovav & D'Arcy as the two groups of authors responsible for the greatest number of publications related to ISec events, with four and three, respectively. Likewise, the research journals publishing the highest number of ISec-event-related articles were *Decision Support System*s and *Computers & Security*, with four and three publications, respectively. Based on the 58 studies evaluated in our analysis, **Fig. 5(a)** depicts the frequency of these publications on an annual basis. In **Fig. 5(b),** we note the publication types and their respective counts. Between 2008 and 2011, we observed an increase in the annual number of publications from one to seven articles. This highlights a possible rise in ISec awareness, corresponding with the period when large organizations began to allocate larger budgets for ISec (Ponemon 2020). In the following four years, we observed a decrease in the publication frequency of ISec-event-related studies; however, research interest increased in 2017, when six publications appeared,

perhaps due to the ISec breaches experienced in that year by Equifax, Goldman Sachs, Verizon, and Weebly, as well as the infamous WannaCry ransomware attack that compromised over 230,000 computers across 150 countries.

Furthermore, researchers have examined market reactions to ISec events by analyzing different types of ISec events. As such, seven types of ISec events were examined and are shown in **Fig. 5(c)**. The major area of interest in the literature was *ISec* b*reaches* (81%), appearing in 47 papers. *Phishing* was analyzed in three papers (5.1%) and *ISec investments* in four papers (6.9%). Finally, events related to *software vulnerabilities*, *IT-security legislation*, *DDOS attacks*, *Heartbleed bugs*,[iii] *and ISec certifications* appeared once each (1.7%).

4.1.2. Major ESM dimensions extracted from papers

We extracted ESM dimensions from the examined papers, and then organized and categorized these features to answer our research questions (**Table A3)**. *First*, we defined the overall timespan covered in all the studies we examined. We labeled this feature *time interval* and found that the earliest period included studies using data in 1988 (P6, P7) and that the latest period was 2018 in P57. Regarding the timespan covered in individual studies, 77% of the studies employed a time interval of five or more years to assess the effects of ISec events on a company's stock performance, with P58 covering the most extended period (22 years, i.e., 1995–2016). Because researchers used varying time intervals to examine ISec events, they could have provided similar accounts of the same ISec event of interest. We thus identified the time intervals covered in every study to note these possible overlaps.

Second, for researchers performing event studies in ISec, one of the most challenging tasks has been to identify enough ISec events to perform meaningful statistical analyses. In our case, to identify possible ISec events, we retrieved studies from the following major *data sources*: Lexis/Nexis, a source commonly used to trace events, was used in 29% of the papers we examined. Another common source was the Data Loss Archive and Database, used in 21% of the papers. Factiva and CNET were used in six and five papers, respectively. We found that since 2014, the Privacy Rights Clearing House has been the most frequently chosen source for ISec-breach studies; it was used in 55% of the papers. Altogether, we found that

researchers used 38 data sources, with 38% of the papers using data obtained from more than one source.

Third, we analyzed the *location of ISec events*, finding that firms headquartered in the US have been the prime sample in most studies assessing the outcomes of market reactions to ISec events, as shown in **Fig. 5(d)**. As such, 45 (75.8%) of the papers examined the phenomenon based solely on stock market indicators of US firms. A major reason to study events related to US-based organizations is that US firms notify clients of ISec incidents as a gesture of good faith to build confidence between stakeholders and organizations. Importantly, the Securities and Exchange Commission (SEC) admonishes companies "to disclose cybersecurity risks and incidents that are material to investors, including the concomitant financial, legal, or reputational consequences" (SEC 2018). Another contributing reason is that material and data from newspaper articles are written in English and are widely accessible to the public. Since 2017, however, 40% of studies have included a mix of US and nonUS firms in their sample. This is likely due to the increasing trend of regulators outside the US also requiring disclosure of ISec events.

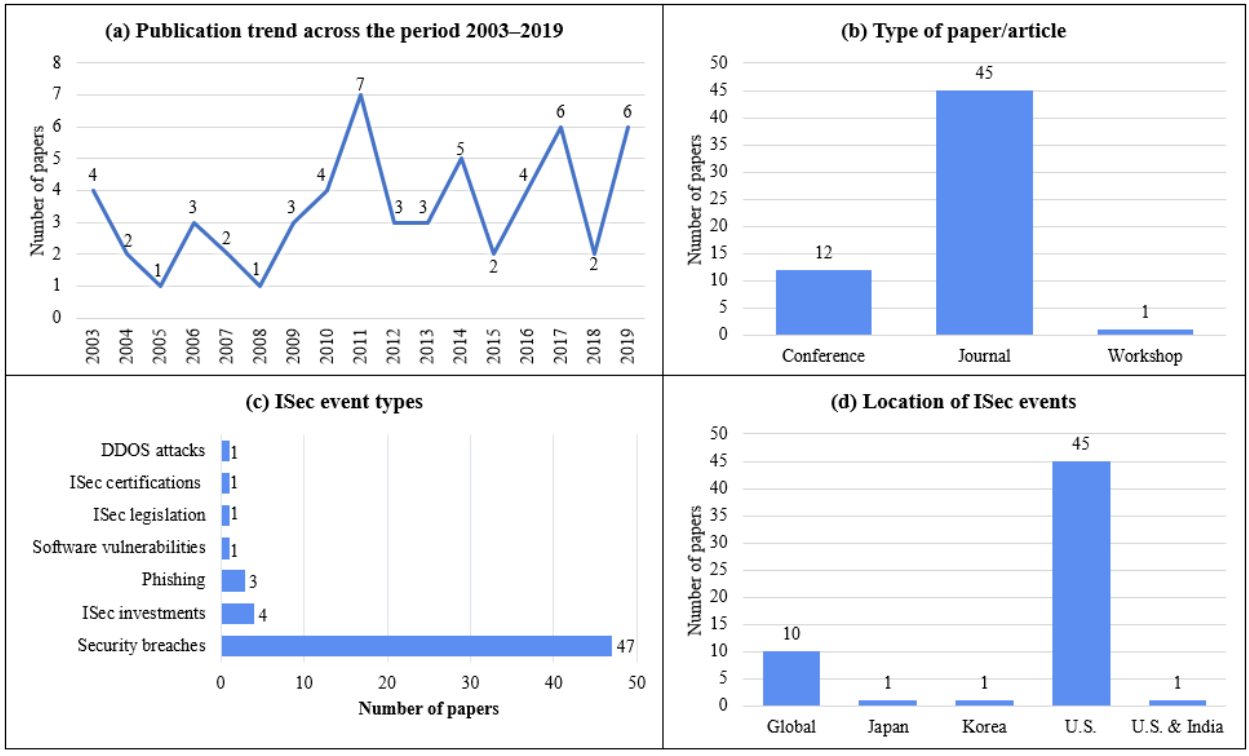

Fig. 5 (a–d). Descriptive characteristics of published papers.

Fourth, about the *estimation model* employed in the studies, the most widely used form (79% of the papers) was the single-factor market model, a model based on the assumption that a stable linear relationship exists between the market return and a firm's stock return. The remaining studies use different versions of the Fama–French three-factor model (Fama and French 1993). This model is based on three factors: market risk, the outperformance of companies with small market capitalizations versus those with large market capitalization, and the outperformance of companies with high book-to-market ratios versus those with low book-to-market ratios. There were other multifactor market models used as well. In P35, the International Fama–French two-factor model, which uses an international book-to-market correction factor (Fama and French 1998) (the difference between high and low book-to-market ratio for each country individually) and the market return, was used; and in P34 and P57, a four-factor estimation model that enhances the momentum factor to the Fama–French three-factor model was employed (also used in P38). We found limited use of international models because most studies used one- or three-factor models to examine the effects of ISec-event announcements on US firms.

Fifth, **Fig. 6** depicts the event sample sizes referenced in each of the papers. The largest event sample size used was in P29 (18,522 phishing events), whereas P4 used the smallest size of four events. The overall average event sample size was 545 events in each study. However, the average sample size was 262 events when studies examined the influence of ISec breaches on the breached firm solely, with 91% of these studies using a sample size of approximately 200 events. Studies of other unfavorable events, such as phishing and the Heartbleed bug (P13, P21, P35, P50), used more than 1000 events for their analysis. Other than P58, a smaller sample size of nearly 100 ISec events was used in studies examining favorable ISec events, such as ISec investments, ISec regulations, and ISec certifications. It can be inferred that favorable ISec events might be more challenging to trace than unfavorable ISec events. We observed smaller sample sizes for studies examining favorable ISec events.

Sixth, the essential element of the ESM is selecting the appropriate *estimation and event windows*, which can affect the statistical significance of CARs. To date, studies have not reached a consensus regarding the appropriate length of these windows. Among the studies we evaluated, we found that the

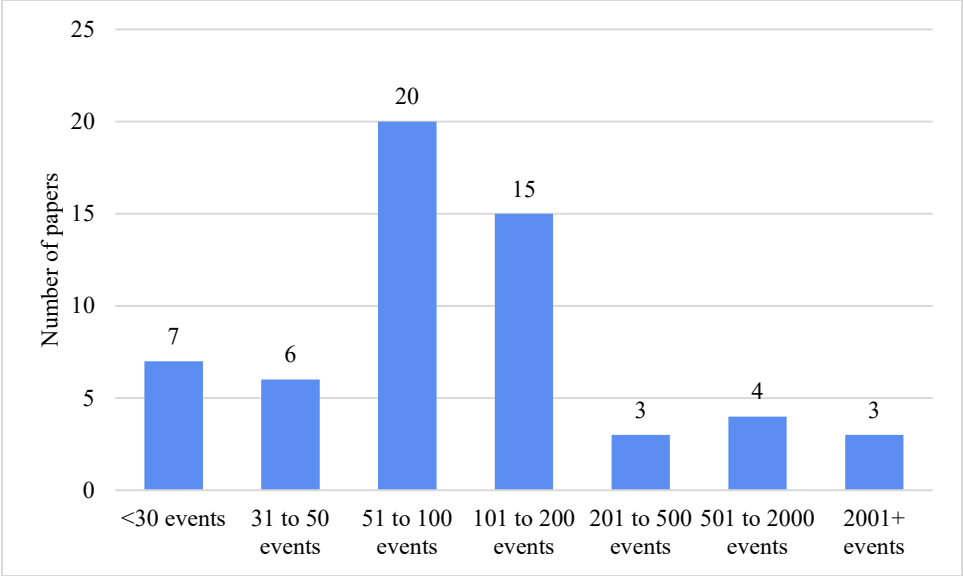

Fig. 6. The event sample size used in papers.

largest estimation window was 299 days (in P51), which started 300 days before the event day and ended one day before the event day. From **Table A3**, the smallest estimation window observed—50 days before the event day—was in P18. In 22% of the papers, the estimation window was greater than 250 days, whereas 19% of the papers had estimation windows of approximately 200 days. We found that another 20% of the papers used an estimation window of 120 days. The purpose of creating an estimation window is to obtain relevant betas and risk premiums from which CARs can be predicted during an event window. Based on a review of estimation windows used by researchers, CARs are predicted based on a timeline of four months to 14 months preceding an ISec event. About event windows, we found that the smallest event window was two days (0, 1) closest to the ISec announcement day as the most common approach (27% of the papers). Approximately 23.5% of the studies incorporated a three-day event window (t = -1, t = 0, t = +1) centered about the announcement day. Moreover, we found that many studies applied more than one event window to test the significance of CARs, with 45.5% of the studies using more than one event window to examine market reactions to ISec events. This means that researchers did not rely on only one event window to conclude the significance of CARs.

Last, to check the significance of CARs, statistical testing is necessary. Studies perform various parametric and nonparametric tests to check the significance of their results **(Table A3)**. Among the

parametric tests, the traditional *t*-test was used in 55% of the papers, whereas 37% of papers employed a *z*-test to examine the significance of CARs. After completing parametric testing, researchers use nonparametric testing to measure the robustness of these outcomes. In event studies, nonparametric tests are a valuable tool for controlling nonnormal distribution and cross-sectional dependence (Chatterjee et al. 2002). However, only 39% of the papers further tested the results of CARs using nonparametric tests. It can be inferred that results based on parametric testing are sufficient to determine the significance of CARs. Among the nonparametric tests, the Wilcoxon signed-rank test (six papers), Corrado's rank *t*-test (five papers), and the sign *z*-test (five papers) were the most used.

4.1.3. Summary results of these studies in terms of stock performance

Table 3 summarizes the results of the reviewed studies. The 58 articles include 80 studies because multiple studies were performed in some papers (i.e., P1, P4, P5, P10, P29, P40, P43, P50, P54, P57, and P58). Seventy-five percent of the studies (60) show that an ISec event significantly influences the company's stock performance, exhibited in most cases by the company's CARs. The consequences of *ISec breaches for breached firms' CARs* represent the most studied phenomenon, with a total of 45 studies (56%). This phenomenon is hypothesized as negative and undesirable.

Accordingly, 32 studies (71%) demonstrate a significant negative influence. Likewise, the influence of other unfavorable events like phishing is also hypothesized to be negative. The results confirm the same hypothesis because two out of the three studies examining the *influence of phishing on related firms' CARs* produce significantly unfavorable or negative results (and the third produced neutral results). Therefore, we can conclude that equity investors batter stocks of firms that experience any type of unfavorable ISec event. Conversely, studies assume that ISec breaches exert a positive influence on *ISec providing firms' CARs*.

The need for advanced ISec measures increases when breaches occur at other firms; three studies examine this relationship and confirm a positive influence. There are inconclusive results regarding the influence of ISec breaches and the CARs of competitors of breached firms. Four studies examine this relationship and find mixed results: A significant positive influence is found in two studies, whereas a significant negative influence is found in the other two. There are five studies on favorable events of firms

Table 3. Summary of the results of the studies we reviewed.

Study type	Influence on . . .	+ (sig.)	+ (not)	- (sig.)	- (not)	Sum (sig.)
Unfavorable ISec events:						
ISec breaches	CARs of breached firms		2	32	11	32
ISec breaches	CARs of competitors of the breached firm	2		3		5
ISec breaches	CARs of ISec firms	3				3
Phishing	CARs of related firms			2	1	2
ISec breaches	CARs of responsible vendors				1	0
Software vulnerabilities	CARs of affected firms			1		1
ISec breaches	CARs of IT consulting firms	1				1
DDOS attacks	CARs of affected firms				1	0
ISec breaches	Trading volume of breached firms	3				3
Phishing	Trading volume of breached firms			1		1
ISec breaches	BAS of breached firms	1				1
Heartbleed	CARs of firms having vulnerable web servers			1		1
Heartbleed	CARs of firms having nonvulnerable web servers			1		1
ISec breaches	Systematic risk of breached firms	1	1			1
ISec breaches	Long-run returns				1	0
						0
Favorable ISec events:						0
ISec legislations	CARs of healthcare firms to which the legislation is applied			1		1
ISec legislation	CARs of ISec firms	1				1
ISec legislation	CARs of IT firms	1				1
ISec investments	CAR of firms making ISec investments	3	1			3
ISec certifications	CARs of firms getting certifications	1				1
ISec investments	CARs of competitors				1	0
ISec investments	Long-run returns	1				1

Header key: + (sig.) = positive direction and significant; **+ (not)** = positive direction but not significant; **- (sig.)** = negative direction and significant; **- (not)** = negative direction but not significant; **sum (sig.)** = total number of significant results (positive or negative)

obtaining ISec certifications (one study), firms making technical ISec investments through ITC measures (two studies), and firms making nontechnical ISec investments (two studies). Of these, four of the five studies find a positive influence, and studies that examine the effect of technical investments in ITC observe a positive effect on the company's stock performance. In nontechnical investments, one study observes a positive effect on company stock performance, while another observes an insignificant effect. Thus, we can conclude that announcements of technical ISec investments are generally more well-received by shareholders and improve the company's stock performance (Wang 2010).

Referring to **Table 3**, we examine 22 distinct types of ISec events in a total of 80 studies. Stock price and resulting CARs are the subjects of 18 of the 22 examinations. *Examinations of ISec breaches that affect*

the stock price of breached firms are still the most common (present in 45 of the 80 studies or 56%), followed by *examinations of competitors of the breached firm* (6%), *examinations of stock performance of ISec firms* (4.5%) (e.g.,, a major ISec breach can lead to significant 4.5% improvement in stock performance of ISec firms such as McAfee, Norton and Symantec subsequent to major ISec breaches) and *examinations of the influence of phishing on related firms* (4.4%).

Additionally, we address research that has appeared in the literature only once, which is illuminating for future research. For instance, a study hypothesizes that *software vulnerabilities on software vendors* and the *effect of ISec breaches on responsible vendors* will result in negative CARs. The latter is insignificant, whereas the former results in significant negative CARs, which corresponds to the DigiNotar (2011) and most recent SolarWinds breaches (2020). As illustration, DigiNotar, a subsidiary of VASCO Data Security International, a Dutch certificate authority, suffered a breach that resulted in the creation of over 500 fraudulent digital certificates for leading internet companies such as Google, Mozilla, and Skype. The company could not recover from this disaster and eventually declared bankruptcy. A recent illustration is the SolarWinds breach, where hackers targeted the company by embedding malicious code into a software update. The company began disseminating the fraudulent certificates to clients' computers between March and June 2020. This resulted in a cyberespionage campaign lasting months and affecting nearly 18,000 organizations worldwide. Even before the company announced its inadvertent complicity in the hack, the stock price plummeted approximately 22%, resulting in a $280 million loss for stockholders. These examples highlight the importance for software vendors to tightly integrate ISec into their software quality practices. Moreover, these cases indicate it is likely better for vendors to more aggressively announce and address these kinds of breaches to preempt possibly worse financial consequences from occurring—for example, increased liability exposure or decreased reputational status.

Other studies appearing only once in the literature include the *effects of newly enacted IT security legislation in the health sector* on the CARs of (1) IT firms, (2) ISec firms, and (3) healthcare firms. CARs are significantly positive for IT and ISec firms but are significantly negative for healthcare firms. Legislation and corporate obligations related to ISec expand revenue for IT and ISec firms but result in

massive expenditures for healthcare firms. Similarly, IT and ISec firms may gain financially from the extra commercial opportunities, which may reflect in the stock performance of IT and ISec firms. However, in the case of healthcare firms, digital transformation may result in negative CARs in the short term, but in the long-term they should profit from IT-enabled organizational transformation, which will improve their value proposition in the long term.

Similarly, two recent studies (P57 and P58) assess the influence of an ISec event on the *long-term stock performance of a firm*. P57 examines the *effect of an ISec breach*, whereas P58 examines the *effect of a firm's ISec investment on identity theft countermeasures (ITC).* P57's results are insignificant. Whereas in P58, significant positive CARs are observed, implying that investments in identity theft countermeasures may result in higher investor trust and possible long-term profits for a company. These one-time studies reveal the importance of empirically investigating phenomena other than the effects of ISec breaches on affected firms.

Finally, we also analyze the magnitude of significant CARs along with the positive or negative effects of ISec-event announcements **(Table A4)**. Studies P1 and P4 observe a higher percentage of negative CARs, averaging -5.5%. In later years, studies P24, P33, P34, and P36 find a significant reduction in negative CARs, but the overall negative CAR averages 3.5% for unfavorable ISec events. In contrast, studies observe a nominal percentage (0.63% to 1.36%) of positive CARs for favorable events, such as ISec investments and ISec certifications (P27, P31, P55, P58). These findings show that stock market reactions to unfavorable ISec events are more volatile than reactions to favorable events. The magnitude of CARs will be higher for unfavorable ISec events in contrast to the magnitude of positive CARs for favorable ISec events. These findings are also consistent with *prospect theory* from behavioral finance, which proposes that people react differently to gains than losses. The psychological effects of experiencing a loss or even facing the possibility of a loss may induce risk-taking behavior, which can increase the likelihood or severity of realized losses (Kahneman and Tversky 2013; Tversky and Kahneman 1992).

4.2. Results for the Level of Stock Market Efficiency

In line with **RQ2**, which examines the efficiency of stock markets as strong, semistrong, or weak for ISec

events, it is necessary to observe the change in stock returns around the event day (i.e., t = 0). We can conclude that a strong form of market efficiency is present if the abnormal returns (ARs) are significant before the event day. Likewise, the semistrong form of market efficiency is concluded if the ARs are significant on the event day or immediately after the day (t = 0, t = +1). Studies assessed these efficiencies through critical observation of CARs and CARs around significant event windows (Khansa et al. 2012; Santos et al. 1993). We found that CARs were most significant during two-day and three-day event windows surrounding the event day (**Fig.7**): the event windows of (0, 1), (0, 2), and (-1, 1) were most significant in 55% of the studies (**Table A4**). Most event windows extending beyond two days of an event are insignificant, except for P49. We thus infer that ISec events affect a company's performance briefly, which signals the presence of strong and semistrong forms of the EMH for ISec-event announcements.

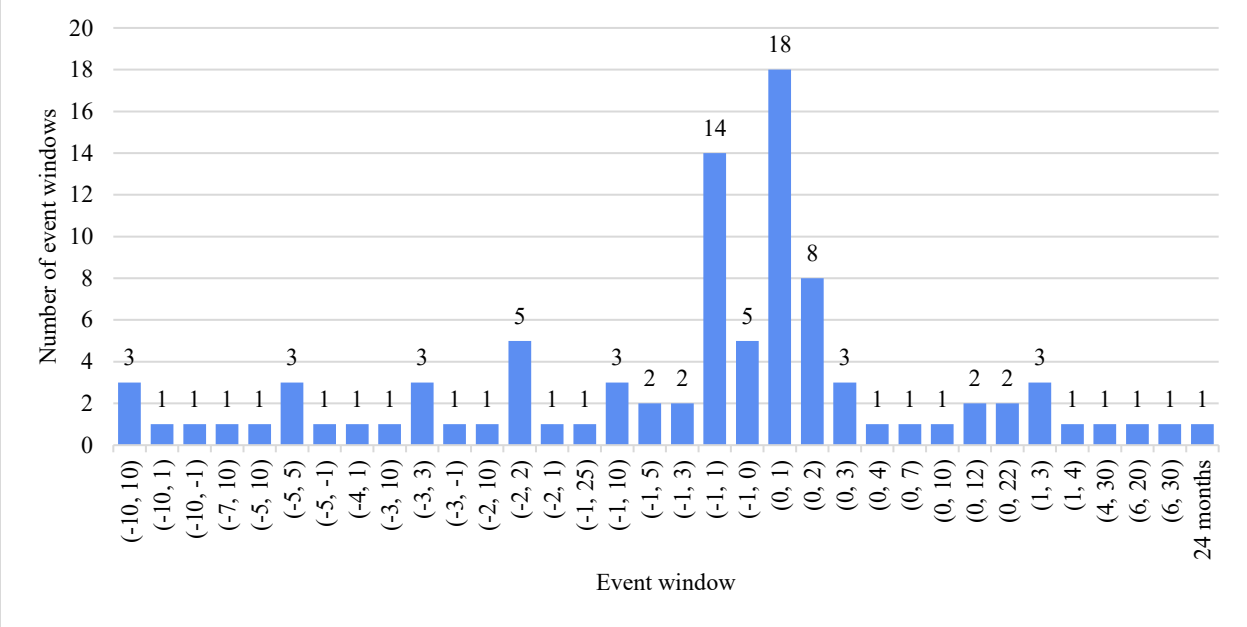

Fig. 7. Frequency of significant event windows concluded in studies.

Another interesting finding is that, in 54% of the studies, significant CARs occur before the event day. This may be the result of insider trading or information leaks in connection with a forthcoming ISec event. Further investigations into favorable and unfavorable ISec events are conducted based on this possibility, in line with the RQ2 of this study. The analysis in **Fig. 8** reveals that 51% and 71% of the significant event windows for unfavorable and favorable ISec events, respectively, began before the event day. These

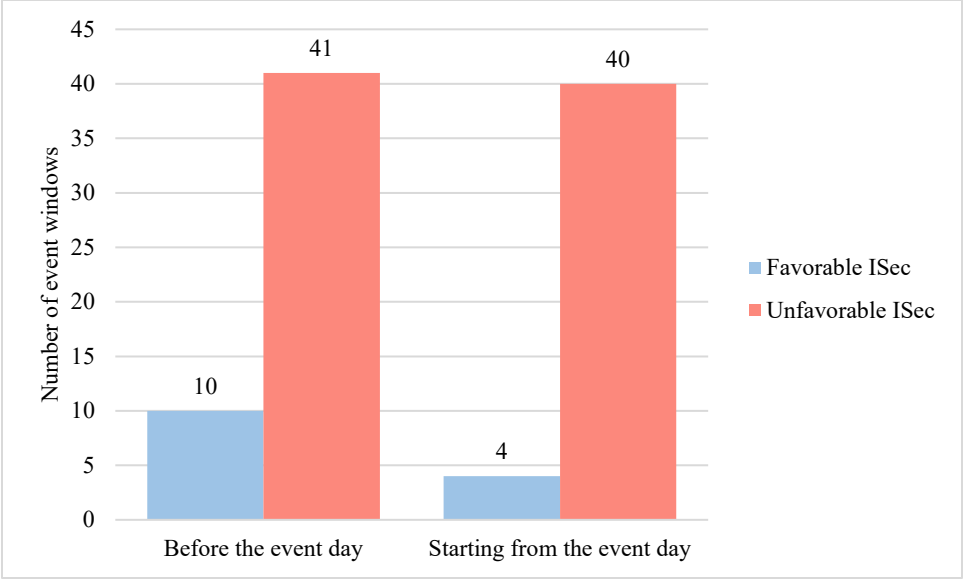

Fig. 8. Frequency of significant CARs before and after the event day.

findings imply that insider trading and information leaks are more prevalent during favorable ISec events than during unfavorable ISec events.[iv] This is sensible, given that firms are traditionally more controlling of information related to negative ISec events.

4.3. Results for ISec Contingency Factors

Table A4 in online Appendix A helps us to answer RQ3, which shows the ISec contingency factors we investigate in the studies. ISec contingency factors explain the change in significant CARs after an ISec event, and 59% of the papers emphasize the influence of ISec contingency factors on market reactions. In other words, researchers find that significant CARs in the stock market are not only a function of event announcements but are also influenced by ISec contingency factors.

We find that *time frame, industry type, type of breach,* and *firm size* are the most significant ISec contingency factors that explain the magnitude of negative CARs associated with unfavorable ISec-event announcements (**Fig. 9**). Regarding time frame, four out of five recent studies conclude that the magnitude of negative CARs is higher for unfavorable ISec events (P5, P17, P22, P24). Firms from technology industries experience higher negative CARs in seven out of 10 studies (P5, P20, P22, P28, P36, P38, P50); the remaining three studies show the same effects for firms in the financial industry (P10, P45, and P52).

We find that five out of seven studies conclude that the type of breach is a significant ISec contingency

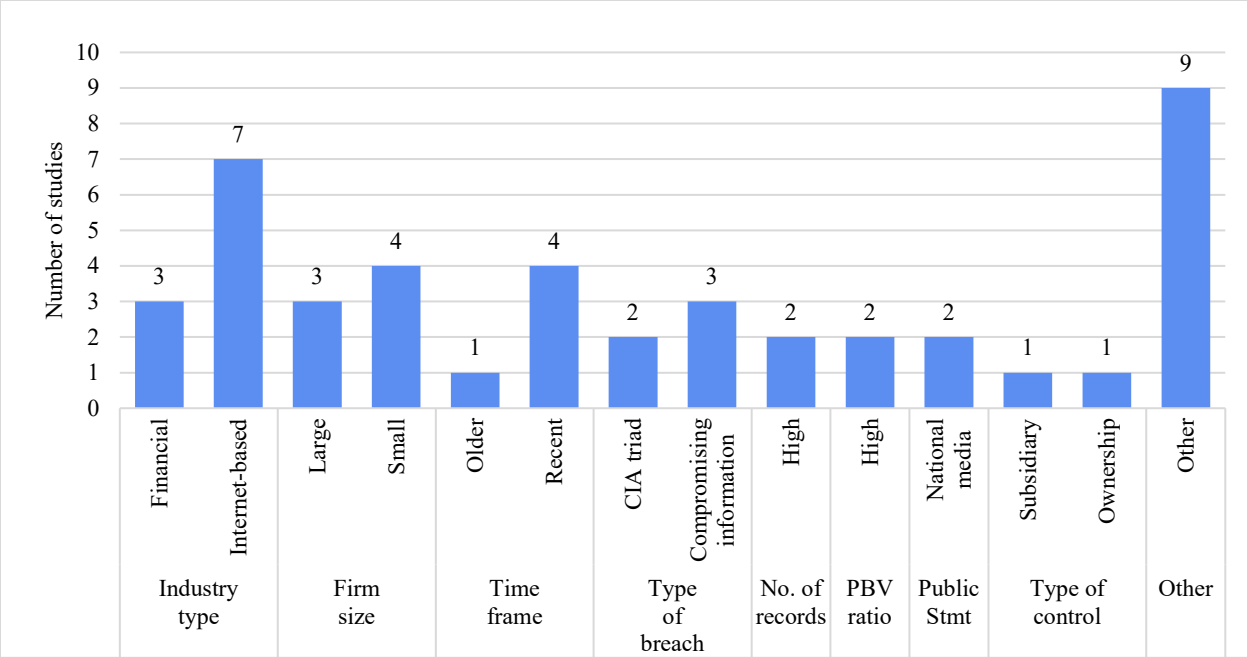

Fig. 9. Key ISec contingency factors as determinants of negative CARs for unfavorable ISec events

factor. Of the five conclusive studies, three find that the magnitude of negative CARs is higher if a breach involves a compromise of confidential information. The remaining two studies find that the violation of the confidentiality, integrity, and availability (CIA) triad leads to a negative CAR.

Firm size is significant in five out of seven studies examining the results of unfavorable ISec events. Among the five studies, three studies (P13, P17, P26) find that large firm size leads to higher negative CARs; however, the other two studies (P9, P38) show contrary results, where smaller firm size leads to higher negative CARs. Based on these findings, we can neither conclude positive nor negative effects of firm size on market reactions to ISec-event announcements.

Regarding favorable ISec occurrences, we could not identify the most relevant ISec contingency factors. Three of the six articles do not examine the role of ISec contingency factors in explaining the CAR. Three other papers (P27, P55, and P58) identify significant ISec contingency factors that vary from one another. We thus surmise that market reactions to favorable ISec events may be directly attributed to the announcement of the event.

4.4. Outcomes Other than Stock Price

Whereas most studies (73) investigate how ISec events affect the stock price, seven examine the influence

of ISec events on stock market factors other than price. In line with RQ4, **Table 2** shows these factors along with the significance of each. For instance, four studies (P30, P31, P33, P48) examine the consequences of ISec breaches on the trading volume of shares for firms making the ISec announcements. Typically, a higher trading volume of shares represents higher stock liquidity and improved investor confidence; however, the increase in trading volume after an ISec-breach announcement usually signals an immediate selling of shares. This, in turn, reduces investor confidence and increases investors' reluctance to make new investments or add to their current positions. Cardenas et al. (2012) advocate trading volume behavior as a signal of information beliefs within a market. If a breach announcement leads to a reduced stock price and increased trading volume, these actions indicate a shared belief among investors regarding a firm's immediate stock performance. However, suppose an ISec breach does not significantly affect the price but creates a significant increase in trading volume. In that case, this indicates the canceling of negative and positive beliefs shared among investors, resulting in a minimal change in stock price. Three out of four studies find that an ISec breach can significantly influence the trading volume. The other study, related to a phishing event (P31), finds that this event causes trading volume to decline significantly. Our findings reveal that ISec-event announcements can significantly influence the trading volume of a publicly traded company.

Table 2. Factors other than price outcomes resulting from ISec events.

Paper no.	Type of IS event	Factor other than price	Price outcome	Sig.
P30	ISec breaches	Trading volume	Positive	Yes
P30	ISec breaches	Systematic risk of the affected firm	Positive	Yes
P31	Phishing	Trading volume	Negative	Yes
P33	ISec breaches	Trading volume	Positive	Yes
P40	ISec breaches	Systematic risk of the affected firm	Positive	No
P48	ISec breaches	BAS	Positive	Yes
P48	ISec breaches	Trading volume	Positive	Yes

Another factor, the systematic risk factor (beta) of a firm, can also be influenced by an ISec-breach announcement (Ali et al. 2020). This research proposes the notion that an ISec breach can have a "contagion effect" that can affect not only the breached firm but also other firms in that sector. For example, P30 shows significant effects of an ISec breach on the systematic risk (beta), whereas P40 yields insignificant effects. P48 examines the effect of ISec-breach announcements on the *bid-ask spread* (BAS). The BAS is the

difference between the maximum price a buyer (trader) is willing to pay for an asset and the lowest price a seller (dealer) is willing to take. Market dealers work with two types of traders: informed and uninformed liquidity traders. *Uninformed* traders transact on public information, whereas *informed* traders transact on information not yet reflected in a company's stock price. P48 inspects this element of informed trading by examining the changes in BAS before and after the ISec-event announcement. The authors conclude that BAS has a one-day abnormal effect and that the same effect is not witnessed before the announcement. They thus conclude that informed market participants do not exploit these events, as Frino et al. (2007) assert.

5. Discussion

The purpose of our SLR was to search for, gather, and categorize event-study articles that address stock market reactions to ISec events. We used a systematic search of bibliographic sources and found 58 relevant papers containing 80 empirical studies. We evaluated the results of these studies regarding the stock market efficiency for ISec events, types of significant ISec contingency factors, and effects on stock market factors other than price.

5.1. Answering the Four Research Questions

We posed **RQ1** to add value to the previous SLR conducted by Spanos and Angelis (2016), by studying and synthesizing the characteristics and results of studies on the influence of ISec events on a company's stock performance. Our SLR covered eight distinct types of ISec events (see **Fig. 5(c)**) and examined 22 distinct types of ISec relationships. We find that 75% of the studies conclude that ISec events significantly influenced company stock performance indicators, primarily price. We also find that unfavorable events, such as ISec breaches and phishing, can decrease a company's stock price by 0.25% to 10%. In contrast, the magnitude of change in stock prices was lower for favorable events, such as ISec investments and certifications (i.e., 0.63% to 1.36%). We thus conclude that unfavorable ISec events lead to more robust market reactions among investors than do favorable ISec events.

We raised **RQ2** to examine the efficiency of stock markets for ISec-related events. We did so by testing the significance of CARs before, during, and after the event/announcement day. We observed a mixture of

strong and semistrong forms of the EMH for markets—primarily in the US: 55% of studies significantly influenced an ISec event within one or two days surrounding the event day. The strong form of EMH is further demonstrated by the fact that CARs for 54% of event windows beginning prior to the event day were significant, suggesting that stock markets react even before an ISec event is announced (**Fig.7**). Our further investigation of favorable ISec events finds that 71% of event windows beginning prior to the announcement day were significant (**Fig.8**). It appears that insider trading or information may be more pervasive during favorable ISec events than during unfavorable ISec events.

We proposed **RQ3** to explore the role of ISec contingency factors in explaining the change in CARs after an ISec event. Based on a thorough extraction of ISec contingency factors and their results from studies, 59% of the papers hypothesize that ISec contingency factors played a role in mediating CARs after an ISec event. Thus, the researchers generally conclude that stock market reactions after an ISec event are a function of these ISec contingency factors. We find the use of ISec contingency factors to be more common in studies examining the effect of unfavorable ISec events on company stock performance. The most significant factors in these studies are time frame, type of industry, type of breach, and firm size.

Finally, we posed **RQ4** to consider the influence of ISec-event announcements on factors other than a company's stock price. Our review reveals that trading volume, BAS, and systematic risk of stock are the nonstock price factors influenced by ISec events. We note other findings from our literature search, including those based on different types of parametric and nonparametric tests used to determine the significance of CARs. We discover that the *t*-test and Corrado's rank test are the most used testing procedures. Last, we show that 45% of the studies use more than one event window to determine the significance of CARs, signaling that authors are not relying on one event window to observe CARs.

The second underlying aim of our SLR was to offer value by exploring new insights not specifically addressed in the SLR by Spanos and Angelis (2016). By addressing RQ1, RQ2, and RQ4, our SLR makes an essential contribution to the body of knowledge, especially by providing vital insights into the EMH, ISec contingency factors, and factors that affect stock price and other nonstock price factors. It has been asserted that stock markets (mostly the US) exhibit a high degree of efficiency in response to favorable ISec

events. Additionally, the degree of a significant CAR relies not only on the event under test but also on ISec contingency factors such as time frame, industry type, breach type, and firm size. Finally, we identify nonprice indicators in the stock market that Spanos and Angelis (2016) may have overlooked or were not available at that time. The general notion is that an ISec event will have a major effect on other stock market indicators such as trade volume, systematic risk, and BAS.

5.2. Contribution to Research and Theory

The studies reviewed in this SLR were based on the EMH, a theory that states that financial markets are informationally efficient and that stock prices reflect all publicly available information. Investors in the stock market consider all available information and evaluate a firm using this information. Accordingly, when new information about an ISec event is publicly released, investors are expected to update their valuations. Studies examine such valuations through the ESM to reveal abnormal trading activity before and during an ISec-event window. Based on a rigorous review of studies and their results, numerous contributions can be made to research and theory.

First, CARs are most significant during two-to-three-day event windows surrounding the event day (**Fig. 6**). Specifically, the event windows (0, 1), (0, 2), and (-1, 1) are the most significant in 55% of the studies. CARs for event windows beyond +2 days tend to be insignificant. Generally, we can conclude that ISec events can affect the stock market performance of firms, but for a brief period.

Second, CARs are significant for 54% of event windows beginning prior to the event day, indicating the presence of both strong and semistrong forms of EMH. Also, CARs are significant for 71 percent of event windows that begin prior to the event day for favorable ISec events. These findings may indicate that forthcoming information about a favorable ISec event has already been leaked into the market prior to the firm's official announcement. If true, this demonstrates a strong form of EMH that indicates the possibility of insider trading or information leaks for favorable ISec events.

Third, the studies observe a lower magnitude of CARs (1%) for favorable ISec events than for unfavorable events (5%). From a theoretical perspective, it can be maintained that markets are more efficient for unfavorable ISec events than for favorable events. Accordingly, firms should continually look

for ways to strengthen their ISec and provide favorable ISec signals, both as a way to strengthen investor confidence but also to prevent actual breaches, which can be more damaging to investor confidence (Nofer et al. 2014).

Fourth, the magnitude of CARs is dependent not only on the ISec-event announcement but also on the ISec contingency factors pertinent to the event. Among the numerous ISec contingency factors, we find that a few, such as breach/attack type, time frame, type of industry, and firm size are significant in most studies. Theoretically, we can thus infer that market efficiency in ISec events will be a function of ISec-event announcements and the firms' ISec contingency factors manifested by the features of context (time frame), industry, event type, and firm assets (firm size).

5.3. Contribution to Practice

Here, we address the practical implications of our SLR results for managers and other policymakers. *First*, the evidence of significant CARs before the announcement of an ISec event signals the presence of the EMH in its strong form. Namely, it signals that the information regarding an ISec event might have already been known to market participants, possibly due to insider trading or information leaks. To gain investors' confidence, firms should implement and enforce a media policy and develop a contingency plan to announce ISec events (Li et al. 2012). Moreover, global policymakers should cooperate on regulatory frameworks by which firms can report ISec events in a standard, systematic manner. For example, the SEC regulates corporations' public disclosure of ISec risks and events and enacts severe penalties on publicly traded companies for lack of complying with its strict guidelines. Additionally, these guidelines are valuable to help firms to anticipate ISec threats and to sufficiently prepare in the likely case they fall victim to an ISec incident (SEC 2018).

Second, identifying significant ISec contingency factors—time frame, industry type, breach type, and firm size—can provide meaningful insights for managers and policymakers. The findings suggest that investors most strongly penalize breached firms when they are smaller in size and from the Internet and technology industry. ISec protocols should therefore be regularly updated, especially for small firms from the technology sector. We also observe heavy penalties on the part of investors where the ISec breach

involves compromising confidential data. ISec-breach attacks are evolving, and cybercriminals are learning new attack methods. Hence, investors are consequently becoming more cautious and concerned about ISec matters. Therefore, the development of cyber-resilient information systems can provide long-term financial gains to a business.

5.4. Post-Spanos and Angelis (2016) Scenario:

The SLR by Spanos and Angelis (2016) was the first and only SLR, until ours, to assess the effects of ISec events on the stock performance of affected firms. Spanos and Angelis analyze and present several factors identified in 47 studies from 37 articles and conclude that ISec events significantly affect stock performance. Their SLR incorporates a variety of relevant facets and dimensions for academics and policymakers. We thus further explain our expanded contributions to their work.

First, one underlying aim of our SLR is to update ISec researchers and practitioners on the evolution of those dimensions as presented by Spanos and Angelis. For example, they identify 11 different study types from 47 events studies, but our expanded SLR identifies 22 different study types from 80 event studies. Clearly, since their SLR was conducted, academics have shown a rising interest in examining the effects of ISec events on other stock market metrics, such as trade volumes, systematic risk, BAS, and long-term stock returns.

Second, an increasing interest in investigating the consequences of ISec events on stock markets outside the US is becoming more prominent in literature since the Spanos and Angelis (2016) SLR was conducted, whereby only 17% of their reviewed publications examined nonUS markets. In our SLR, this percentage grew to 25 percent, and after 2017, 40% of all articles included samples involving data from nonUS firms. This trend is important as policymakers worldwide are increasingly regulating disclosures of ISec events.

Third, the Privacy Rights Clearinghouse (PRCH) emerged as a major data source for ISec event studies, with 55% of all articles citing this source. According to Spanos and Angelis (2016), PRCH was used as a data source in fewer than 10% of their reviewed papers. Collecting a sufficient sample size for analysis has been difficult for ISec researchers. However, the ability to easily retrieve data from the PRCH has clearly aided ISec researchers immensely in their data collection efforts.

Fourth, and likely aided by the PRCH, the average event sample size has nearly tripled since Spanos and Angelis (2016) conducted their study. For example, in their study, the average number of events examined for the most prevalent type of event (i.e., ISec breaches to breached firms) was 92. In our updated SLR, this average increased to 262 events—demonstrating that ISec breaches are rising in frequency and data about the breach events are more readily available than before.

5.5. Limitations and Future Research Opportunities

Despite its value, our SLR has several limitations that point to future research opportunities. *First,* our review incorporated all studies that employed the ESM, which is designed to examine the visible effects of an ISec incident on a company's stock performance. However, ISec events could have other long-term negative and positive consequences on a firm's performance through indicators, such as on return-on-assets, price-to-earnings ratio, IT strategic alignment, number of returning customers, market share, brand image, and corporate governance. The ESM is inadequate for investigating the long-term effects on such indicators. Such research may require the gathering of a mix of longitudinal primary and secondary data.

Second, the set of papers extracted for this review were from the relevant sources of WOS, Scopus, Science Direct, and Google Scholar, all of which are among the most relevant and prestigious sources in the academic environment. Contributions from other outlets (e.g., working papers) were not included, even though they may have relevance to this review. The advantage of future research including working papers is the ability to capture emerging topics; the disadvantage is they have not been vetted through peer-review.

Third, the influence of ISec events on stock market indicators other than price is an understudied area. Only seven studies (8.75%) examine the influence of ISec events on indicators other than the stock price. Despite having significant results for unfavorable ISec events, these other stock indicators have yet to attract real attention from researchers in the context of favorable ISec events. For instance, the effects of ISec breaches on BAS are significantly positive. An unexpected ISec breach can create an arbitrage opportunity for informed traders who know which market makers are reluctant to increase their spread. Accordingly, it would be useful to examine the consequences of favorable events for these stock market indicators and how such favorable events can affect the decision-making of traders and dealers.

Fourth, a major research avenue exists concerning the financial consequences of regulators' announcements of ISec regulations or frameworks. Khansa et al. (2012) (P29) attempt to examine the influence of such announcements, as they investigate the effects of ISec legislation on the market value of firms in the healthcare sector. Researchers can examine the economic consequences of ISec legislation in other vulnerable sectors, such as Internet-based firms and firms in the financial and energy sectors. For example, ISec legislation can provide long-term assurances of ISec and can require hefty investments from firms to pay for system upgrades, team member training, and more (Ali et al. 2021a).

Fifth, relatively few studies examine the influence of favorable ISec events. Considering the shifting landscape, numerous avenues abound for examining the influence of favorable ISec events and their subsequent influence on a company's financial performance, including stock performance and other measures not frequently studied in event studies (e.g., brand image). For example, future studies could examine the stock market reaction to companies' announcements regarding their participation in information sharing and analysis centers (ISACs), outsourcing ISec processes to a security firm, or red team evaluations. We believe an especially crucial favorable ISec event to consider are various strategic cyberthreat intelligence initiatives that are emerging throughout industry and government (Shin and Lowry 2020; Wagner et al. 2019).

Our SLR also provides several future research opportunities. *First*, the convergence of the digital, biological, physical, and new technologies, such as cloud computing, next-generation robotics, 3D printing, the Internet of Things, and improved wireless technologies is revolutionizing business practices and workflows. Today, data virtualization is considered a part of the digital transformation concept. Unfortunately, the broad use of digital technologies, from commerce to social connections to business, also increases the prevalence of cybercrime. Cybercrimes are expected to exceed traditional crimes in cost and number (Anderson et al. 2019; Netherlands 2020; Ventures 2019), due to their low risk and high return nature. Because of the shifting world of cyberattacks and ISec, it behooves researchers to provide updated comprehensive SLRs to keep industry and academia apprised of continually developing trends, attack vectors, and protective ISec behaviors and programs.

Second, these transformations have altered the way companies view their ISec governance and have illuminated the importance of understanding the financial implications related to ISec events, especially those implication such as ISec breaches influencing key leading stock market indicators. Reports show that ISec breaches are rising in prevalence and magnitude, costing companies, governments, and citizens a staggering $6 trillion in losses in 2021, up from $3 trillion in 2015 (Hiscox 2021). Thus, the capacity to address ISec issues proactively is critical for preserving an organization's competitive edge—in terms of economic growth and market position strengthening (Barbier et al. 2016; Shin and Lowry 2020; Wagner et al. 2019). Further, ISec strategies should be appropriately linked with organizational, governmental, and information technology strategies to improve an organization's overall performance (Waslo et al. 2017).

Third, given the rapid digital transformations occurring within organizations, catalyzed partly by the COVID-19 pandemic as a titanic shock event, we find it imperative to integrate digital transformation research with ISec research to anticipate the evolution of cyberattacks. Namely, Wessel et al. (2021) distinguish between IT-enabled organizational transformation and digital transformation. Wynn Jr and Williams (2020) reexamine the idea of digital infrastructure, whereas Adesemowo (2021) discusses information technology assets and digital technologies. Further, Baskerville et al. (2020) extend the discussion by highlighting the ontological reversal of digital technologies. The factors identified by these teams of researchers will influence the trends in digital technologies and, ultimately, the perspective ISec researchers may have on new, plausible types of data breaches and ISec events and their subsequent influences on stock market values and returns. Using an integrated lens, future researchers can envision new pathways to examine the effects of digitization developments on the financial performance of concerned organizations.

6. Conclusion

Previous literature reviews have provided valuable insights into ISec events and the research trends and financial consequences of such events. However, these reviews did not analyze the association between ISec events and key company financial measures related to a company's stock performance. Consequently, we conducted an SLR to examine the effects of ISec events on company stock price performance. We

included an analysis of market efficiency for ISec events, ISec contingency factors, and factors other than the stock price. Besides confirming the effect of ISec events on the company's stock performance, our SLR has profound implications for academics, managers, and policymakers. We also note that there is still an opportunity for further research to investigate the effects of ISec events on other aspects of investment decision-making. Specifically, managers must recognize the gravity of ISec events and the distinct types of ISec events that lead to financial consequences for businesses and their shareholders. These avenues serve as future research opportunities. Our findings provide ISec and management scholars with a foundation they can build upon to make more profound and widespread contributions to theory and practice in their respective fields.

Acknowledgments

(Blinded for peer review).

References

Adebayo AO (2012) A foundation for breach data analysis. *Journal of Information Engineering Applications* 2(4):17-23.

Adesemowo AK (2021) Towards a conceptual definition for IT assets through interrogating their nature and epistemic uncertainties. *Computers & Security* 105(June):102131.

AICPA (2015) Security regains place as top technology priority for CPAs, North American survey finds.

Al-Emran M, Mezhuyev V, Kamaludin A (2018) Technology acceptance model in M-learning context: A systematic review. *Computers & Education* 125(October):389-412.

Ali RF, Dominic P, Ali SEA, Rehman M, Sohail A (2021a) Information security behavior and information security policy compliance: A systematic literature review for identifying the transformation process from noncompliance to compliance. *Applied Sciences* 11(8):3383.

Ali SEA, Lai F-W, Hassan R, Shad MK (2021b) The long-run impact of information security breach announcements on investors' confidence: The context of efficient market hypothesis. *Sustainability* 13(3):1066.

Ali SEA, Lai F-WL, Hassan R (2020) Socio-economic factors on sector-wide systematic risk of information security breaches: Conceptual framework. In: *9th International Economics and Business Management Conference*, European Proceedings of Social and Behavioural Sciences, Melaka, Malaysia:502-512.

Almadhoun NM, Dominic PDD, Woon LF (2011) Perceived security, privacy, and trust concerns within social networking sites: The role of Information sharing and relationships development in the Malaysian higher education institutions' marketing. In: *International Conference on Control System, Computing and Engineering*, IEEE, Penang, Malaysia:426-431.

Anderson R, Barton C, Bölme R, Clayton R, Ganán C, Grasso T, Levi M, Moore T, Vasek M (2019) Measuring the changing cost of cybercrime.

Arcuri MC, Brogi M, Gandolfi G (2014) The effect of information security breaches on stock returns: Is the cyber crime a threat to firms? In: *European Financial Management Meeting*, Citeseer, Italy 1-12.

Arcuri MC, Brogi M, Gandolfi G (2017) How does cyber crime affect firms? The effect of information security breaches on stock returns. In: *First Italian Conference on Cybersecurity*, Venice, Italy:175-193.

Barbier J, Buckalew L, Loucks J, Moriarty R, O'Connell K, Riegel M (2016) Cybersecurity as a growth advantage. CISCO.

Baskerville RL, Myers MD, Yoo Y (2020) Digital first: The ontological reversal and new challenges for IS research. *MIS Quarterly* 44(2):509-523.
Bezerra F, Favacho CH, Souza R, de Souza CRB (2014) Towards supporting systematic mappings studies: An automatic snowballing approach. In: *29th SBBD Conference*, Curitiba, Brazil:167-176.
Boell SK, Cecez-Kecmanovic D (2015) On being `systematic'in literature reviews. *Formulating Research Methods for Information Systems* (Palgrave Macmillan, London) 48-78.
Bose I, Leung ACM (2013) The impact of adoption of identity theft countermeasures on firm value. *Decision Support Systems* 55(3):753-763.
Bose I, Leung ACM (2014) Do phishing alerts impact global corporations? A firm value analysis. *Decision Support Systems.* 64(August):67-78.
Bose I, Leung ACM (2019) Adoption of identity theft countermeasures and its short and long-term impact on firm value. *MIS Quarterly* 43(1):313-327.
Broadbent M, Weill P, Neo BS (1999) Strategic context and patterns of IT infrastructure capability. *Journal of Strategic Information Systems* 8(2, June):157-187.
Campbell K, Gordon LA, Loeb MP, Zhou L (2003) The economic cost of publicly announced information security breaches: Empirical evidence from the stock market. *Journal of Computer Security* 11(3):431-448.
Cao J, Calderon T, Chandra A, Wang L (2010) Analyzing late SEC filings for differential impacts of IS and accounting issues. *International Journal of Accounting Information Systems* 11(3, September):189-207.
Cardenas J, Nicholas-Donald A, Coronado AS, Parra F, Mahmood MA (2012) The economic impact of security breaches on publicly traded corporations: An empirical investigation. In: *18th Americas Conference on Information Systems*, SEA, US:1393-1400.
Cavusoglu H, Mishra B, Raghunathan S (2004) The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. *International Journal of Electronic Commerce* 9(1):70-104.
Chai S, Kim M, Rao HR (2011) Firms' information security investment decisions: Stock market evidence of investors' behavior. *Decision Support Systems* 50(4, March):651-661.
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.
Chatterjee D, Pacini C, Sambamurthy V (2002) The shareholder-wealth and trading-volume effects of information-technology infrastructure investments. *Journal of Management Information Systems* 19(2):7-42.
Chen X, Bose I, Leung ACM, Guo C (2011) Assessing the severity of phishing attacks: A hybrid data mining approach. *Decision Support Systems* 50(4, March):662-672.
Collins A (2018) The global risks report 2018. World Economic Forum, Geneva.
Collins A (2019) The global risks report 2019. World Economic Forum, Geneva.
Dardan M, Dardan S (2005) The valuation of eCommerce announcements during fluctuating financial markets. *Journal of Electronic Commerce Research* 6(4):312-327.
De Groot J (2019) The history of data breaches. In: *Digital Guardian*.
Deane JK, Goldberg DM, Rakes TR, Rees LP (2019) The effect of information security certification announcements on the market value of the firm. *Information Technology and Management* 20(3):107-121.
Dehning B, Richardson VJ, Zmud RW (2003) The value relevance of announcements of transformational information technology investments. *MIS Quarterly* 27(4):637-656.
Ding L, Lam HK, Cheng T, Zhou H (2018) A review of short-term event studies in operations and supply chain management. *International Journal of Production Economics* 200 (June):329-342.
Dong K, Ali RF, Dominic P, Ali SEA (2021) The effect of organizational information security climate on information security policy compliance: The mediating effect of social bonding towards healthcare nurses. *Sustainability* 13(5):2800.
Eling M, Schnell W (2016) What do we know about cyber risk and cyber risk insurance? *Journal of Risk*

Finance 17(5):474-491.
Ettredge M, Richardson VJ (2002) Assessing the risk in eCommerce. In: *Annual Hawaii International Conference on System Sciences*, IEEE, Hawaii, US:1-11.
Fama EF (1991) Efficient capital markets: II. *The Journal of Finance* 46(5):1575-1617.
Fama EF, French KR (1993) Common risk factors in the returns on stocks and bonds. *Journal of Financial Economics* 33(1, February):3-56.
Fama EF, French KR (1998) Value versus growth: The international evidence. *Journal of Finance* 53(6):1975-1999.
Frino A, Jones S, Wong JB (2007) Market behaviour around bankruptcy announcements: Evidence from the Australian stock exchange. *Accounting and Finance.* 47(4):713-730.
Garg A, Curtis J, Halper H (2003) The financial impact of IT security breaches: What do investors think? *Information Systems Security* 12(1):22-33.
Goel S, Shawky HA (2009) Estimating the market impact of security breach announcements on firm values. *Information & Management* 46(7, October):404-410.
Goldstein J, Chernobai A, Benaroch M (2011) An event study analysis of the economic impact of IT operational risk and its subcategories. *Journal of the Association for Information Systems* 12(9):606-631.
Gordon LA, Loeb MP, Sohail T (2010) Market value of voluntary disclosures concerning information security. *MIS Quarterly* 34(3):567-594.
Hayden E (2013) Data breach protection requires new barriers. In: *TechTarget*.
Hina S, Panneer Selvam DDD, Lowry PB (2019) Institutional governance and protection motivation: Theoretical insights into shaping employees' security compliance behavior in higher education institutions in the developing world. *Computers & Security* 87(Article: 101594.
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, April):337-347.
Hiscox (2021) Cyber readiness report: Don't let cyber be a game of chance.
Hovav A, D'Arcy J (2003) The impact of denial-of-service attack announcements on the market value of firms. *Risk Managment and Insurance Review* 6(2):97-121.
Hovav A, D'Arcy J (2004) The impact of virus attack announcements on the market value of firms. *Information Systems Security* 13(3):32-40.
Hovav A, D'Arcy J (2005) Capital market reaction to defective IT products: The case of computer viruses. *Computers & Security* 24(August):409-424.
Hovav A, Han JY, Kim J (2017) Market reaction to security breach announcements: Evidence from South Korea. *Data Base for Advances in Information Systems* 48(1):11-52.
Hsu C, Lee JN, Straub DW (2012) Institutional influences on information systems security innovations. *Information Systems Research* 23(3-2):918-939.
Im KS, Dow KE, Grover V (2001) Research report: A reexamination of IT investment and the market value of the firm - An event study methodology. *Information Systems Research* 12(1):103-117.
Imran M, Arif T, Shoaib MJ (2018) A statistical and theoretical analysis of cyberthreats and its impact on industries. *International Journal of Scientific Research in Computer Science Applications and Management Studies* 7(5):1-7.
Jansen J, Junger M, Montoya L, Hartel P (2013) Offenders in a digitized society. *Cybercrime and the Police* (Eleven International Publishing, Hague, ND) 45-59.
Janze C (2017) Intruder alert? How stock markets react to potential IT secuirty breachs: The case of openSSL heartbleed. In: *30th BLED Econference: Digital Transformation-from Connecting Things to Transforming Our Lives* Bled EConference p. 33, Bled Slovenia:245-264.
Jeong CY, Lee SYT, Lim JH (2019) Information security breaches and IT security investments: Impacts on competitors. *Information & Management* 56(5, July):681-695.
Kahneman D, Tversky A (2013) Prospect theory: An analysis of decision under risk. *Handbook of the fundamentals of financial decision making: Part I* (World Scientific) 99-127.
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.
Khan KS, Kunz R, Kleijnen J, Antes G (2003) Five steps to conducting a systematic review. *Journal of the Royal Society of Medicine* 96(3):118-121.
Khansa L, Cook DF, James T, Bruyaka O (2012) Impact of HIPAA provisions on the stock market value of healthcare institutions, and information security and other information technology firms. *Computers & Security.* 31(6, September):750-770.
Khansa L, Liginlal D (2011) Predicting stock market returns from malicious attacks: A comparative analysis of vector autoregression and time-delayed neural networks. *Decision Support Systems* 51(4):745-759.
Kim JY (2013) Analyzing effects on firms' market value of personal information security breaches. *Journal of Society for e-Business Studies* 18(1):1-12.
Kitchenham B (2004) Procedures for performing systematic literature reviews. Joint Technical Report, Keele University TR/SE-0401 and NICTA TR-0400011T.1, Keele, UK:33-33.
Kitchenham B, Charters S (2007) Guidelines for performing systematic literature reviews in software engineering EBSE Technical Report Keele University & University of Durham, Keele, UK.
Konchitchki Y, O'Leary DE (2011) Event study methodologies in information systems research. *International Journal of Accounting Information Systems* 12(2, June):99-115.
Kwon J, Johnson ME (2015) Protecting patient data-the economic perspective of healthcare security. *IEEE Security & Privacy* 13(5):90-95.
Li C, Peters GF, Richardson VJ, Watson MW (2012) The consequences of information technology control weaknesses on management information systems: The case of sarbanes-oxley internal control reports. *MIS Quarterly* 36(1):179-203.
Liginlal D, Sim I, Khansa L (2009) How significant is human error as a cause of privacy breaches? An empirical study and a framework for error management. *Computers & Securty* 28(3, May):215-228.
Lowry PB (2018) An emerging scholar's guide to the leading international information systems and business analytics reseaerch resources and publication outlets. *Working Paper, Department of Business Information Technology, Pamplin College of Business, Virginia Tech, VA, US* Department of Business Information Technology, Pamplin College of Buisness, Virginia Tech, VA, US:SSRN (https://doi.org/10.2139/ssrn.3252222; accessed
Lowry PB, Cao J, Everard A (2011) Privacy concerns versus desire for interpersonal awareness in driving the use of self-disclosure technologies: The case of instant messaging in two cultures. *Journal of Management Information Systems* 27(4):163-200.
Lowry PB, Dinev T, Willison R (2017) Why security and privacy research lies at the centre of the information systems (IS) artefact: proposing a bold research agenda. *European Journal of Information Systems* 26(6):546-563.
Lukonga I (2018) Fintech, inclusive growth and cyber risks: Focus on the MENAP and CCA regions. *IMF Working Papers* 18 (
MacKinlay AC (1997) Event studies in economics and finance. *Journal of Economic Literature* 35(1):13-39.
Malkiel BG, Fama EF (1970) Efficient capital markets: A review of theory and empirical work. *Journal of Finance* 25(2):383-417.
Masaki Ishiguro HT, Kanta Matsuura (2006) The effect of information security incidents on corporate values in the Japanese stock market. In: *International Workshop on the Economics of Securing the Information Infrastructure* 1-15.
Morse EA, Raval V, Wingender JR (2011) Market price effects of data security breaches: A global perspective. *Information Security Journal* 20(6):263-273.
Netherlands C (2020) Less traditional crime, more cybercrime.
Njenga K, Lowry PB (2018) Information security policy violations: A grounded theory approach to counterfactual balance and tensions. In: *Dewald Roode Workshop in Information Systems Security*, Cape Town:14-15.
Nofer M, Hinz O, Muntermann J, Roßnagel H (2014) The economic impact of privacy violations and

security breaches. *Businees & Information Systems Engineering* 6(6):339-348.
Pelletier JM (2017) Effects of data breaches on sector-wide systematic risk in financial, technology, healthcare and services sectors. In: *ProQuest Dissertations and Theses*, Thesis submitted to Capella University:104.
Petticrew M, Roberts H (2008) *Systematic reviews in the social sciences: A practical guide,* , (Blackwell Publishing., MA, USA).
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, November):257-271.
Ponemon (2020) Percentage of total IT budgets spent on IT security from FY2005 to FY2017. Ponemon Institutue: Thales Group.
Protiviti (2016) Executive perspectives on top risks for 2016.
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(January):146-154.
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(September):458-469.
Roztocki N, Weistroffer H (2011) Event studies in information systems research: Past, present and future. *European Conference on Information Systems (ECIS)*June 10.
Roztocki N, Weistroffer HR (2008) Event studies in information systems research: A Review. *Proceedings of the Fourteenth Americas Conference on Information Systems*, Toronto, ON, Canada), August 14-17, 1-10.
Roztocki N, Weistroffer HR (2009a) Event studies in information systems research: An updated review. In: *15th Americas Conference on Information Systems*, SF, USA:1528-1537.
Roztocki N, Weistroffer HR (2009b) Stock market reaction to information technology investments: Towards an explanatory model. In: *17th European Conference on Information Systems.*, Ver, Italy:883-894.
Santos BLD, Peffers K, Mauer DC (1993) The impact of information technology investment announcements on the market value of the firm. *Information Systems Research* 4(1):1-23.
Schwartz RA (1970) Efficient capital markets: A review of theory and empirical work: Discussion. *The Journal of Finance* 25(2):421-423.
SEC (2018) Commission statement and guidance on public company cybersecurity disclosures,. SEC.
Shahzad K, Nawab RMA, Abid A, Sharif K, Ali F, Aslam F, Mazhar A (2019) A process model collection and gold standard correspondences for process model matching. *IEEE Access* 7(30708-30723.
Shiller RJ (2000) Measuring bubble expectations and investor confidence. *Journal of Psychology and Financial Markets* 1(1):49-60.
Shin B, Lowry PB (2020) A review and theoretical explanation of the 'Cyberthreat-Intelligence (CTI) capability' that needs to be fostered in information security practitioners and how this can be accomplished. *Computers & Security* 92(May):Article: 101761.
Sinanaj G, Muntermann J (2013) Assessing corporate reputational damage of data breaches: An empirical analysis. In: *26th Bled EConference - EInnovations Challenges and Impacts for Individuals, Organizations and Society*, Bled, Slovenia:78-89.
Smith KT, Smith LM, Smith JL (2011) Case studies of cybercrime and their impact on marketing activity and shareholder value. *Academy of Marketing Studies Journal* 15(2):67-82.
Spanos G, Angelis L (2016) The impact of information security events to the stock market: A systematic literature review. *Computers & Securty* 58(May):216-229.
Tversky A, Kahneman D (1992) Advances in prospect theory: Cumulative representation of uncertainty. *Journal of Risk and Uncertainty* 5(4):297-323.
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.

Ventures C (2019) Official annual cybercrime report.
Wagner TD, Mahbub K, Palomar E, Abdallah AE (2019) Cyber threat intelligence sharing: Survey and research directions. *Computers & Security* 87(Article: 101589.
Wang P (2010) Chasing the hottest IT: Effects of information technology fashion on organizations. *MIS Quarterly* 34(1):63-85.
Wang T, Kannan KN, Ulmer JR (2013) The association between the disclosure and the realization of information security risk factors. *Information Systems Research* 24(2):201-218.
Waslo R, Lewis T, Hajj R, Carton R (2017) Industry 4.0 and cybersecurity: Managing risk in an age of connected production. Deloitte University Press.
Wessel L, Baiyere A, Ologeanu-Taddei R, Cha J, Blegind-Jensen T (2021) Unpacking the difference between digital transformation and IT-enabled organizational transformation. *Journal of the Association for Information Systems* 22(1):102-129.
Wynn Jr DE, Williams CK (2020) Recent advances and opportunities for improving critical realism-based case study research in IS. *Journal of the Association for Information Systems* 21(1):8.
Yayla AA, 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.
Yun H, Lee G, Kim DJ (2019) A chronological review of empirical research on personal information privacy concerns: An analysis of contexts and research constructs. *Information & Management* 56(4, June):570-601.
Zafar H, Ko M, Osei-Bryson K-M (2012) Financial impact of information security breaches on breached firms and their non-breached competitors. *Information Resources Management Journal* 25(1):21-37.
Zafar H, Ko MS, Osei-Bryson K-M (2016) The value of the CIO in the top management team on performance in the case of information security breaches. *Information Systems Frontiers* 18(6):1205-1215.
Zhang L, Huang J (2009) The review of empirical researches on IT investment announcements on the market value of firms. *International Journal of Business and Management* 4(10):14-27.

[i] Our reference to stock performance is in the context of equity share price performance, which includes the fluctuation of equity prices of any given company listed on either the NASDAQ or New York Stock Exchange or any other stock exchange. These equities are traded vehicles and are commonly referred to as "common stock," a form of corporate equity ownership that can be freely traded in secondary markets, such as in the stock exchanges.

[ii] *Random walk* is an earlier theory of efficient markets. The basic assumptions here is that the current price of a security fully reflects publicly available information and that price changes are independent and identically distributed. This would imply that past movements in stock prices cannot predict future movements in stock prices.

[iii] The Heartbleed bug is a hazardous vulnerability in OpenSSL cryptographic software library that can allow the attacker to steal the protected information.

[iv] We are grateful to our anonymous reviewer for recommending that we analyze market efficiency for both positive and negative ISec occurrences. We observed a novel finding as a result, which helped to improve the value of the manuscript. We appreciate the reviewer's insightful comment.

Online Appendix A. Literature Review Detailed Support

Table A1. Articles excluded from the current systematic review and why they were excluded.

Paper	Author(s) (Year)	Type of paper	Name of journal/conference	Major findings	Reason for exclusion
E1	Kwon and Kim (2007)	Journal	*Information Systems Review*	n/a	Article in Korean language.
E2	Gordon et al. (2010)	Journal	*MIS Quarterly*	Voluntarily disclosing items concerning information security is associated positively with the market value of a firm.	This study focuses on voluntary ISec disclosures by firms during annual filings. Event study methodology not used.
E3	Khansa and Liginlal (2011)	Journal	*Decision Support System*	Prediction of returns of ISec firms through VAR and time-delayed neural networks	Event study methodology not used.
E4	Kim (2013)	Anonymous	*Anonymous*	An analysis of stock price change and information management	Article in the Korean Language.
E5	Hovav and Gray (2014)	Journal	*Communications of the Association for Information Systems*	The study employs a stakeholder analysis and finds that, while some stakeholders are losers, others are winners. The analysis also implies that, depending on subsequent events, the effect of a security breach on the attacked firm varies over time, suggesting a "wait and see" attitude by the market.	This study explores the in-depth analysis of a one breach incident of TJX. Includes an event study together with the longitudinal method of security events for TJX.
E6	Gwebu et al. (2014)	Conference	*Pacific Asia Conference on Information Systems*	ISec breaches negatively influence firm profitability, perceived risk, and information transparency. Nevertheless, the losses associated with direct costs such as compensation and litigation costs will be higher as compared to indirect costs such as tarnished reputation and a decrease in market share and sales.	Event study method not used.
E7	Nofer et al. (2014)	Journal	*Business & Information Systems Engineering*	By using a lab experiment, by the first-order effect, it is found that general security breaches more severely damaged the investor's trust as compared to privacy violations.	The event study method not used. Primary data analysis by experiment in a laboratory.

Paper	Author(s) (Year)	Type of paper	Name of journal/conference	Major findings	Reason for exclusion
E8	Kwon and Johnson (2014)	Journal	*MIS Quarterly*	Voluntarily proactive security investments are associated with lower security failure rates than reactive investments.	The study is about the effect of security investment on reducing security failures instead of on stock performance. Thus, no event study methodology was used.
E9	Kwon and Johnson (2015)	Journal	*IEEE Security and Privacy*	An economic perspective has been presented about the vulnerability of data breaches in the health care sector.	No empirical examination has been conducted for the influence of data breaches on stock performance.
E10	Hsu et al. (2016)	Conference	*Hawaii International Conference on System Sciences*	No influence on firm performance (ROA & Stock Returns) after ISO 27001 certification.	Event study methodology not used.
E11	Szubartowicz and Schryen (2020)	Working Paper	n/a	The stock price will react more positively to a firm's announcement of actual information security investments than to announcements of the intention to invest. The stock price will react more positively to a firm's announcements of actual information security investments after the fundamental security incident compared to before.	Working papers not included in our analysis.
E12	Corbet and Gurdgiev (2019)	Journal	*International Review of Financial Analysis*	This study examines the influence of cybercrime and hacking events on equity market volatility across firms. It is found that volatility will be dependent on the type of breach event, hacking, large data breaches, and the number of clients exposed.	Event study methodology not used.

Table A2. Articles included in the systematic literature review, with number cross-referencing.

Paper no.	Citation	Type of paper	Source	Type of ISec event examined
P1	Garg et al. (2003)	Journal	*Information Management and Computer Security*	Security breaches
P2	Campbell et al. (2003)	Journal	*Journal of Computer Security*	Security breaches
P3	Hovav and D'Arcy (2003)	Journal	*Risk Management and Insurance Review*	Security breaches
P4	Ettredge and Richardson (2003)	Journal	*Journal of Information Systems*	Security breaches
P5	Cavusoglu et al. (2004)	Journal	*International Journal of Electronic Commerce*	Security breaches
P6	Hovav and D'Arcy (2004)	Journal	*Information Systems Security*	Security breaches
P7	Hovav and D'Arcy (2005)	Journal	*Computers & Security*	Security breaches
P8	Acquisti et al. (2006)	Conference	*International Conference on Information Systems*	Security breaches
P9	Masaki Ishiguro (2006)	Workshop	*International Workshop on the Economics of Securing the Information Infrastructure*	Security breaches
P10	Aytes et al. (2006)	Conference	*Americas Conference on Information Systems*	Security breaches
P11	Telang and Wattal (2007)	Journal	*IEEE Transactions on Software Engineering*	Software vulnerabilities
P12	Kannan et al. (2007)	Journal	*International Journal of Electronic Commerce*	Security breaches
P13	Bose and Leung (2008)	Conference	*International Conference on Information Systems*	Phishing
P14	Goel and Shawky (2009)	Journal	*Information & Management*	Security breaches
P15	Muntermann and Roßnagel (2009)	Conference	*Nordic Conference on Computer Security*	Security breaches
P16	Liginlal et al. (2009)	Journal	*Computers & Security*	Security breaches
P17	Gatzlaff and McCullough (2010)	Journal	*Risk Management and Insurance Review*	Security breaches
P18	Patel (2010)	Journal	*Duke Journal of Economics*	Security breaches
P19	Bolster et al. (2010)	Journal	*Journal of Business Valuation and Economic Loss Analysis*	Security breaches
P20	Andoh-Baidoo et al. (2010)	Journal	*IEEE Security & Privacy*	Security breaches
P21	Chen et al. (2011)	Journal	*Decision Support Systems*	Phishing
P22	Yayla and Hu (2011)	Journal	*Journal of Information Technology*	Security breaches
P23	Smith et al. (2011)	Journal	*Academy of Marketing Studies*	Security breaches
P24	Morse et al. (2011)	Journal	*Information Security Journal*	Security breaches
P25	Gordon et al. (2011)	Journal	*Journal of Computer Security*	Security breaches
P26	Malhotra and Kubowicz Malhotra (2011)	Journal	*Journal of Service Research*	Security breaches
P27	Chai et al. (2011)	Journal	*Decision Support Systems*	Information security investments
P28	Chen et al. (2012)	Journal	*Computers in Human Behavior*	Security breaches
P29	Khansa et al. (2012)	Journal	*Computers & Security*	IT security legislation
P30	Cardenas et al. (2012)	Conference	*Americas Conference on Information Systems*	Security breaches
P31	Bose and Leung (2013)	Journal	*Decision Support Systems*	Identity theft counter measures
P32	Sinanaj and Muntermann (2013)	Conference	*Bled eConference*	Security breaches

Paper no.	Citation	Type of paper	Source	Type of ISec event examined
P33	Wang et al. (2013)	Journal	*Journal of Organizational Computing and Electronic Commerce*	Security breaches
P34	Goel and Shawky (2014)	Journal	*Communications of the Association for Information Systems*	Security breaches
P35	Bose and Leung (2014)	Journal	*Decision Support Systems*	Phishing
P36	Pirounias et al. (2014)	Journal	*Journal of Information Security and Applications*	Security breaches
P37	Arcuri et al. (2014)	Conference	*European Financial Management Association Meeting*	Security breaches
P38	Das et al. (2012)	Journal	*Journal of Information Privacy and Security*	Security breaches
P39	Modi et al. (2015)	Journal	*Journal of Operations Management*	Security breaches
P40	Hinz et al. (2015)	Journal	*Information & Management*	Security breaches
P41	Schatz and Bashroush (2016)	Journal	*Information & Computer Security*	Security breaches
P42	Chen et al. (2016)	Conference	*IOP Conference Series: Materials Science and Engineering*	Security breaches
P43	Martin et al. (2017)	Journal	*Journal of Marketing*	Security breaches
P44	Sinanaj and Zafar (2016)	Conference	*Pacific Asia Conference on Information Systems*	Security breaches
P45	Arcuri et al. (2017)	Conference	*Italian Conference on Cyber Security*	Security breaches
P46	Johnson et al. (2017)	Journal	*Journal of Finance Issues*	Security breaches
P47	Abhishta et al. (2017)	Conference	*Euromicro International Conference on Parallel, Distributed and Network-Based Processing*	DDOS attacks
P48	Rosati et al. (2017)	Journal	*International Review of Financial Analysis*	Security breaches
P49	Hovav et al. (2017)	Journal	*Data Base for Advances in Information Systems*	Security breaches
P50	Janze (2017)	Conference	*Bled eConference*	Security breaches
P51	Patsakis et al. (2018)	Journal	*Computers & Security*	Security breaches
P52	Tweneboah-Kodua et al. (2018)	Journal	*Information & Computer Security*	Security breaches
P53	Richardson et al. (2019)	Journal	*Journal of Information, Communication and Ethics in Society*	Security breaches
P54	Jeong et al. (2019)	Journal	*Information & Management*	Security breaches/ISec investments
P55	Deane et al. (2019)	Journal	*Information & Technology Management*	Information security certifications
P56	Rosati et al. (2019)	Journal	*Research in International Business and Finance*	Security breaches
P57	Richardson et al. (2019)	Journal	*Journal of Information Systems*	Security breaches
P58	Bose and Leung (2019)	Journal	*MIS Quarterly*	Identity theft counter measures

Table A3. Key methodology choices for each included paper.

No.	Time interval	Data source	Estimation model	Location	Estimation window	Event window	Parametric tests	Non-parametric tests
P1	1996–2002	Bloomberg, Dow Jones Interactive	One factor	US	Not reported	(0, 2)	*t*-test	Wilcoxon signed rank
P2	1995–2001	*Wall Street Journal, New York Times, Washington Post, Financial Times, USA Today*	One factor	US	(-123, -2)	(-1, 1)	*z*-test	Not reported
P3	1998–2002	Lexis/Nexis	One factor	US	(-203, -2)	(-1, 0), (-1, 1), (1, 5), (-1, 10), (-1, 25)	*z*-test	n/a
P4	2000	Not reported	One factor	US	(-300, -45)	(0,3), (0, 6)	*t*-test	Wilcoxon signed rank
P5	1996–2001	Lexis/Nexis, CNET, ZDNET	One factor	US	(-160, -1)	(0, 1)	*t*-test	Wilcoxon signed rank
P6	1988–2002	Lexis/Nexis	One factor	US	Not reported	(0, 0), (0, 1), (0, 5), (0, 10), (0, 25)	*z*-test	n/a
P7	1988–2002	Lexis/Nexis	One factor	US	(-201, -2)	(0, 1), (0, 5), (0, 10), (0, 25)	*z*-test, *t*-test	n/a
P8	2000–2006	Lexis/Nexis, ProQuest, Choice point, Data Loss Archive and Database, www.emergentchaos.com	One factor	US	(-100, 8)	(0, 1)	*t*-test	Not reported
P9	2002–2005	Nippon Keizai Shinbun, Nikkei Sangyo Shinbun, Nikkei Ryutsu Shinbun, Nikkei Kinyu Shinbun	One factor	Japan	Not reported	(-1, 38)	*t*-test	Not reported
P10	1995–2005	Lexis/Nexis	One factor	US	(-151, -31)	(-2, 2)	*t*-test	n/a
P11	1999–2004	Lexis/Nexis	One factor	US	(-175 , -16)	(0, 1)	*t*-test	Wilcoxon signed rank
P12	1997–2003	*Wall Street Journal, New York Times,* ZDNET, CNet	One factor	US	(-50, -2)	(-1, 2), (-1, 7), (-1, 29)	*t*-test	n/a
P13	2003–2007	Milermiles, Factiva, MyCERT, Hong Kong Monetary Authority, Antiphishing Group Japan	One factor	Global	(-230, 30)	(-2, 2)	*z*-test	Not reported
P14	2004–2008	Lexis/Nexis, *Wall Street Journal, PC Week*, Register	Three factor	US	(-375, -120)	(-119, 10)	*t*-test	Not reported
P15	2001–2007	Data Loss Archive and Database	One factor	US	(-286, -31)	(-5, 5)	*z*-test	Wilcoxon signed rank

No.	Time interval	Data source	Estimation model	Location	Estimation window	Event window	Parametric tests	Non-parametric tests
P16	2005–2008	Privacy Rights Clearing House, Data Loss Archive and Database, Google, *New York Times, Washington Post*	One factor	US	(-78, -3)	(-2, 9)	*t*-test	Not reported
P17	2004–2006	LexisNexis database, Privacy Rights Clearing House	One factor	Global	(-252, -7)	(0, 1)	*z*-test	Not reported
P18	–	Data Loss Archive and Database	One factor	US	(50, 0)	(0, 2), (0, 7), (0, 29)	Not reported	Not reported
P19	2000–2007	Prowess/Capitaline databases, Data Loss Archive and Database (www.capitaline.com)	One factor	US	(-301, -46)	(-1, 0), (-1, 1), (1, 30)	Not reported	n/a
P20	1997–2003	Lexis/Nexis	One factor	US	(-121, -2)	(-1, 1)	*z*-test	Not reported
P21	2005–2008	Millersmiles	One factor	Global	(-230, -30)	(-1, 1)	Not reported	n/a
P22	1994–2006	Lexis/Nexis	One factor	US	(-130, -10)	(-1, 1), (-1, 5), (-1, 10)	*t*-test	Corrado rank
P23	2000–2005	ProQuest	One factor	US	Not reported	(0, 1), (0, 3)	*t*-test	Not reported
P24	2000–2010	Data Loss Archive and Database	One factor	US	(-505, -251)	(0, 1)	*z*-test	Not reported
P25	1995–2007	*Wall Street Journal, New York Times, Washington Post, Financial Times, USA Today*	One factor, three factor	US	(-123, -2)	(-1, 1)	*z*-test	Not reported
P26	2000–2007	Attrition.org	four factor	US	(-201, -1)	(-1, 1), (2, 30)	*z*-test	Sign Z test, Corrado rank
P27	1997–2006	Lexis/Nexis	One factor	US	(-300, -45)	(-1,1), (-2, 2), (-1, 0), (0, 1)	*t*-test	Corrado rank
P28	2006–2007	Data Loss Archive and Database	One factor	US	(-200, -30)	(-1, 1)	Not reported	Not reported
P29	1996–2010	Public Health Data Standards	One factor	US	(-130, 30)	(-1, 10), (-2, 10), (-3, 10), (-5, 10), (-7, 10), (-10,10)	*t*-test	n/a
P30	2002–2008	Lexis/Nexis	One factor	US	(-251, -1)	(0, 1)	*t*-test	n/a
P31	1995–2012	Factiva, PR Newswire, Business Newswire	One factor	US	(-230, -30)	(0, 1)	*z*-test	Sign Z test
P32	2004–2011	Data Loss DB	One factor	Mainly US	(-150, -50)	(-5, 5)	*t*-test	Not reported
P33	1997–2008	Factiva, CNet, ZDNet & Yahoo!	One factor	US	(-300, -45)	(-1, 1)	Not reported	Not reported
P34	2001–2008	Privacy Rights Clearing House	One factor, four factor	US	(-255, 0)	(-30, 30)	*z*-test	Not reported

No.	Time interval	Data source	Estimation model	Location	Estimation window	Event window	Parametric tests	Non-parametric tests
P35	2003–2007	Millersmiles, Factiva, MyCERT, Hong Kong Monetary Authority, Antiphishing group Japan	One factor, Two factor	Global	(-230, -30)	(-1, 0), (0, 1), (-1, 1)	*z*-test	Sign Z test
P36	2008–2012	ITRC, PRCH, Data Loss Archive and Database	Three factor	US	(-201, -2)	(-1, 0, 1)	*t*-test	Not reported
P37	1995–2012	Factiva	One factor	US	(-122, -1)	(-20, 20), (-10; 10), (-5; 5), (-3; 3), (-1, 1)	*z*-test	Not reported
P38	2000–2012	PRCH	Three factor	US & India	(-122, -2)	(-1, 1), (-1, 3)	*t*-test	n/a
P39	1995–2012	Factiva	One factor	US	(-265, -10)	(-2, 2)	*t*-test	Generalized sign, Wilcoxon signed rank
P40	2011–2012	Data Loss Archive and Database	One factor	Global	(-200, 0)	(0, 1), (0, 2), (0, 3), (0, 5)	*t*-test, *z*-test,	J-test
P41	2005–2014	PRCH	One factor	US	(-121, -1)	(-1, 1), (0, 0), (1, 5), (-1, 5)	*t*-test	n/a
P42	2005–2014	PRCH	One factor	US	(-121, -3)	(-2, 2)	*t*-test	Generalized sign, Wilcoxon signed rank
P43	2006–2015	Capital IQ, Factiva, Lexis-Nexis, and PRCH	One factor	Global	(-270, -6)	(-1, 1)	*t*-test	Wilcoxon signed rank
P44	2011–2013	Data Loss DB	One factor	Global	(-44, -2)	(-1, 10)	*t*-test	n/a
P45	1995-2015	PRCH	One factor	US	(21, 141)	(-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)	*z*-test, *t*-test	Sign test
P46	2005–2014	PRCH	One factor	US	(-285, -30)	(0, 2)	*t*-test	Not reported
P47	2010–2015	Various	Three factor	US	(-202, -2)	(-1, 0), (-1, 1), (-1, 3), (-1, 5), (-1, 10)	*z*-test	n/a
P48	2005–2014	PRCH	Bid ask	US	(-132, -6)	(-5, 5)	*t*-test	Not reported

No.	Time interval	Data source	Estimation model	Location	Estimation window	Event window	Parametric tests	Non-parametric tests
P49	2001–2011	PRCH	One factor	Korea	(-202, -2)	(-1, 0), (-1, 1), (-1, 5), (-1, 10), (-1, 25)	*z*-test	Not reported
P50	2013–2014	Not reported	One factor	Global	(-201, -1)	(0, 2), (0, 12), (0, 22)	*z*-test	G rank t-test
P51	2013–2015	Bloomberg, Reuters	One factor, three factor	US	(-300, -1)	(0, 3)	*z*-test	n/a
P52	2013–2017	BLI, Yahoo finance	One factor	US	(-260, -11)	(-30, 30)	*t*-test	n/a
P53	2011-2014	ProQuest	One factor	US	Not reported	(-1, 1), (-3, 3), (-7, 7)	*t*-test	n/a
P54	2010–2017	Lexis/Nexis, PRCH, Datalossdb.org, ITRC, Heritage	One factor	US	(-182, -2)	(-2, 2), (-1, 1), (0, 1), (0, 2)	*t*-test	Not reported
P55	2005–2015	BSI Group Database	One factor, three factor	US	(-295, -40)	(-1, 0)	*t*-test	Not reported
P56	2011–2014	PRCH, Lexis/Nexis	One factor	US	(-125, -6)	(0, 1), (0, 2), (0, 3), (4, 10)	*t*-test	Not reported
P57	2004-2018	PRCH, Audit Analytics	Four factor	Global	(-120, -5)	(-1, 21)	*t*-test	Corrado rank, Generalized sign test
P58	1995-2016	Factiva	Three factor	Global	(-233, -33)	(-1,0), (0,1), (1,1)	*z*-test	Sign test, Corrado rank

Table A4. ISec contingency factors and results for each included study.

No.	Study focus	Events	Results	Significant event window	Significant ISec contingency factors	In-significant ISec contingency factors
P1	ISec breaches on abnormal returns (CARs) of breached firms	22	Sig. negative (5.6%)	(0, 2)	Higher negative influence for security breaches affecting confidential information.	n/a
P1	ISec breaches on CARs of IS firms	22	Sig. positive (0.9% to 3.3%)	(0, 2)	Not examined	Not examined
P2	ISec breaches on CARs of breached firms	43	Insignificant*	n/a	n/a	n/a
P3	ISec breaches on CARs of breached firms	23	Insignificant*	n/a	n/a	n/a
P4	ISec breaches on CARs of breached firms	4	Sig. negative (-5.19%)	(1, 3)	Higher negative influence for large size firms as compared to small size firms.	n/a
P4	ISec breaches on CARs of ISec firms	10	Sig. positive (15.68%)	(1, 3)	Not examined	Not examined
P4	ISec breaches on CARs of breached firm's competitors	168	Sig. negative (-3.43%)	(1, 3)	Not examined	Not examined
P5	ISec breaches on CARs of breached firms	66	Sig. negative (-2.1%)	(0, 1)	Higher negative influence if the firms have: 1) higher Internet dependence, 2) small size, and 3) suffered a breach in recent times.	Type of attack
P5	ISec breaches on CARs of ISec firms	66	Sig. positive (3%)	(0, 1)	n/a	Type of attack
P6	ISec breaches on CARs of breached firms	186	Insignificant*	n/a	n/a	n/a
P7	ISec breaches on CARs of responsible vendors	92	Insignificant*	n/a	n/a	n/a
P8	ISec breaches on CARs of ISec firms	79	Sig. negative (-.58%)	(0, 1)	Higher negative influence if: 1) breaches are reported through national media and 2) large number of individuals are affected by the breach.	n/a
P9	ISec breaches on CARs of ISec firms	70	Sig. negative (-1.89%)	(0, 10)	Higher negative influence for firms having a higher PBV ratio.	Firm size, Affected information (CIA), Industry type
P10	ISec breaches on CARs of breached firms	67	Insignificant*	n/a	n/a	n/a

No.	Study focus	Events	Results	Significant event window	Significant ISec contingency factors	In-significant ISec contingency factors
P10	ISec breaches on CARs of breached firms' competitors	67	Sig. positive (0.79%)	(-2, 2)	Not examined	Not examined
P11	Software vulnerabilities and CARs of announcing firms	147	Sig. negative (-0.65%)	(0, 1)	Higher negative influence if 1) the location of the product is competitive or if the vendor is small and 2) there is a presence of the patch.	Breaches affecting confidentiality, vulnerability discovered by whom
P12	ISec breaches on CARs of breached firms	72	Insignificant*	n/a	n/a	n/a
P13	Phishing to related firms	2994	Sig. negative (5.1%)	(-1, 1)	Higher negative influence if the breached firm 1) has a large size and 2) is a holding firm.	Place of incorporation, time
P14	ISec breaches to CARs of breached firms	168	Sig. negative (-1.1%)	(-4, 1)	Not examined	Not examined
P15	ISec breaches to CARs of breached firms	97	Sig. negative (-0.42%)	(0, 1)	n/a	Six different business types (weakly supported)
P16	ISec breaches to CARs of breached firms	151	Sig. negative (-0.59% to -0.72%)	(-2, 1), (-2, 2)	Not examined	Not examined
P17	ISec breaches to CARs of breached firms	77	Sig. negative (-.46%)	(-1, 0)	Higher negative influence if: 1) firm size is large, 2) firm is subsidiary, 3) market to book ratio is higher, 4) time is recent, and 5) the firm refused to answer questions about the data breach in initial news report.	Confidential, Number of records
P18	ISec breaches to CARs of breached firms	34	Sig. negative (-2.27%)	(0, 7)	Not examined	Not examined
P19	ISec breaches to CARs of breached firms	93	Insignificant*	n/a	n/a	n/a
P20	ISec breaches to CARs of breached firms	41	Sig. negative (3.18%)	(-1, 1)	Higher negative influence if 1) firm has internet dependence, 2) breaches occur after Feb. 2000, and 3) source of an attack is outside the firm.	n/a
P21	Phishing to CARs of related firms	1030	Insignificant*	(-1, 1)	n/a	Characteristics (insig.)
P22	ISec breaches to CARs of breached firms	123	Sig. negative (-0.92% to -1.61%)	(-1, 1), (-1, 5), (-1, 10)	Higher negative influence if: 1) the firm is purely e-commerce based, 2) the attack type is DOS, and 3) the breach is of more recent time.	Industry type, Technology firm

No.	Study focus	Events	Results	Significant event window	Significant ISec contingency factors	In-significant ISec contingency factors
P23	ISec breaches to CARs of breached firms	10	Sig. negative (-2.2% to 3.5%)	(1, 4)	Not examined	Not examined
P24	ISec breaches to CARs of breached firms	306	Sig. negative (-0.28%)	(0, 1)	Higher negative influence if: 1) breach source is stolen laptop, 2) fraudulent access & hacking, and 3) breach occurs in recent times.	n/a
P25	ISec breaches to CARs of breached firms	121	Sig. negative (-1.36%)	(-1, 1)	Higher negative influence if: 1) the breach compromises the CIA triad and 2) it occurred before the 9/11 incident.	n/a
P26	ISec breaches to CARs of breached firms	93	Sig. negative (-0.78% to -1.92%)	(-5, 5), (-3, 3), (-10, 10), (4, 30), (6, 20), (6, 30)	Higher negative influence for large-size firms.	n/a
P27	ISec investments to CARs of firms that invest	101	Sig. positive (1.01% to 1.36%)	(-1, 1), (-2, 2), (-1, 0), (0, 1)	Higher positive influence if: 1) ISec investment is for commercial exploitation and 2) legislation relates to Sarbanes–Oxley Act (SOX).	Firm size
P28	ISec breaches to CARs of IT consulting firms	77	Sig. positive (0.08%)	(0, 1)	Higher negative influence for IT consulting firm if: 1) many records are breached and 2) the breach occurs in the technology/retail sector.	n/a
P29	ISec legislations to CARs of health firms to whom legislation is applied	2095	Sig. negative (-1.66% to -1.15%)	(-1, 10), (-2, 10), (-3, 10), (-5, 10), (-7, 10), (-10, 10)	Not examined	Not examined
P29	ISec legislation to CARs of IT firms	18522	Sig. positive (0.95% to 1.49%)		Not examined	Not examined
P29	ISec legislation to CARs of ISec firms	1653	Sig. positive (1.05% to 1.98%)		Not examined	Not examined
P30	ISec breaches to CARs of breached firms	39	Insignificant*	n/a	n/a	n/a
P31	ISec measures to CARs of firms that announce ISec measures	87	Sig. positive (-.63%)	(0, 1)	Not examined	Not examined
P32	ISec breaches to CARs of breached firms	72	Sig. negative (0.72% to 1.55%)	(0, 1), (0, 3), (0, 4)	Not examined	Not examined
P33	ISec breaches to CARs of breached firms	89	Sig. negative (-0.15%)	(-1, 1)	Higher negative influence if the textual contents around the breach provide more detailed information regarding the incidents.	n/a

No.	Study focus	Events	Results	Significant event window	Significant ISec contingency factors	In-significant ISec contingency factors
P34	ISec breaches to CARs of breached firms	201	Sig. negative (-0.63%)	(0, 1)	Not examined	Not examined
P35	Phishing to CARs of related firms	1942	Sig. negative (-0.01% to -0.05%)	(0, 1), (-1, 0)	Higher positive influence if the firms have: 1) higher growth potential, 2) higher credit ratings, and 3) history of early adopters of sophisticated measures.	n/a
P36	ISec breaches to CARs of breached firms	105	Sig. negative (-0.39%)	(-1, 0)	Higher negative influence for firms that belong to the technology sector.	n/a
P37	ISec breaches to CARs of breached firms	128	Sig. negative (-0.3% to -1.2%)	(-5, 5), (-3, 3), (-1, 1)	Not examined	Not examined
P38	ISec breaches to CARs of breached firms	101	Sig. negative (-1.15% to -1.51%)	(-1,1), (-1,3)	Higher negative influence if: 1) firm has small size, 2) firm type is internet-specific, 3) breach has serious damage potential, 4) type of attack is theft of confidential information, and 5) firm has lower revenue earnings	Subsidiary firm
P39	ISec breaches to CARs of breached firms	128	Sig. negative (-1.17%)	(-1, 1)	Higher negative influence if: 1) breach is triadic and 2) employee productivity is low.	Financial leverage
P40	ISec breaches to CARs of breached firms	6	Sig. negative (-1.16% to -4.06%)	(0, 1), (0, 2), (0, 3)	Not examined	Not examined
P40	ISec breaches to CARs of competitors of breached firm	346	Sig. negative (-0.19% to -0.9%)	(0, 1), (0, 2), (0, 3)	Not examined	Not examined
P41	ISec breaches to CARs of breached firms	120	Insignificant*	n/a	n/a	n/a
P42	ISec breaches to CARs of breached firms	50	Sig. negative (-2.38%)	(-2, 2)	Higher negative influence if a breach is repeated to the same organization.	n/a
P43	ISec breaches to CARs of breached firms	414	Sig. negative (-0.29%)	(-1, 1)	Higher negative influence if 1) firms show low transparency for data management and 2) firms offer lower control.	n/a
P43	ISec breaches to CARs of competitors of breached firm	414	Sig. negative (-0.17%)	(-1, 1)	Not examined	Not examined
P43	ISec breaches to CARs of competitors of breached firm	414	Sig. negative (-0.17%)	(-1, 1)	Not examined	Not examined
P44	Data breaches to CARs of breached firms	28	Insignificant*	n/a	n/a	n/a

No.	Study focus	Events	Results	Significant event window	Significant ISec contingency factors	In-significant ISec contingency factors
P45	ISec breaches to CARs of breached firms	226	Sig. negative (-3.32% to -0.23%)	(-10, 1), (-10, 10), (-5, 5), (-3, 3), (-10, -1), (-5, -1), (-3, -1)	Higher negative influence if: 1) non-confidential information is compromised and 2) the firm is from the financial industry.	n/a
P46	ISec breaches to CARs of breached firms	467	Sig. negative (-0.37%)	(0, 2)	Higher negative influence if: 1) breach type is payment card fraud and 2) more records are lost.	Repeated breaches, Firm type (Retail/Financial)
P47	DDOS attacks on effected firms' CARs	35	Insignificant*	n/a	n/a	n/a
P48	ISec breaches to CARs of breached firms	74	Sig. negative (-2.53%)	(0, 1)	Higher positive influence on trading volume and bid-ask spread when the breaches have high influence.	n/a
P49	ISec breaches to CARs of breached firms	105	Sig. negative (-0.34% to -0.39%)	(-1, 5), (-1, 10), (-1, 25)	Higher negative influence if: 1) after a few days of the announcement and 2) the industries are regulated.	n/a
P50	Heartbleed announcements to the abnormal returns of firms having non-vulnerable webservers	537	Sig. negative (-2.94% to -5.28%)	(0, 12), (0, 22)	Higher negative influence on consumer discretionary and health care industry	n/a
P50	Heartbleed announcement to unaffected firms' abnormal returns of firms having vulnerable webservers	1638	Sig. negative (-2.5% to -4.3%)	(0, 12), (0, 22)	Higher negative influence for communication, technology, and health care industry	n/a
P51	ISec breaches to CARs of breached firms	80	Insignificant*	n/a	n/a	n/a
P52	ISec breaches to CARs of breached firms	96	Insignificant*, mixed	n/a	Higher negative influence for firms from financial industry.	n/a
P53	ISec breaches to CARs of breached firms	10	Insignificant*	n/a	n/a	n/a
P54	ISec breaches to CARs of breached firms	118	Sig. negative, (-0.251% to -0.42%)	(-2, 2), (-1, 1), (0, 1), (0, 2)	Not examined	Not examined
P54	IT security investments to CARs of firms that invest	98	Insignificant*	n/a	n/a	n/a
P54	ISec breaches to CARs of competitors of breached firm	118	Sig. positive (0.207%)	(0, 2)	Not examined	Not examined

No.	Study focus	Events	Results	Significant event window	Significant ISec contingency factors	In-significant ISec contingency factors
P54	ISec investment to CARs of non-investment making firms	98	Insignificant*	n/a	n/a	n/a
P55	ISec certifications to CARs of firms getting certifications	111	Sig. positive (0.72%)	(-1, 0)	Higher positive influence if: 1) the firms are from the financial and manufacturing industry and 2) firm size is small.	n/a
P56	ISec breaches to CARs of breached firms	87	Sig. negative (-.8% to -1.6%)	(0, 1), (0, 2)	Higher negative influence if: 1) there is higher social media exposure at the time of the data breach and 2) media visibility is traditional.	n/a
P57	ISec breaches to breached firms' short-run returns	827	Sig. negative (0.3%)	(-1,3)	n/a	n/a
P57	ISec breaches to breached firms' long-run returns	827	Insignificant*	n/a	n/a	n/a
P58	ITC measures to CARs of investing firms	526	Sig. positive (0.58%)	(0,1)	Higher short-term positive influence if: 1) the firm is listed in U.S., 2) the firm is an early adopter of ITC, and 3) the firm adopts a government-advocated sophisticated ITC.	
P58	ITC measures to long-run returns	526	Sig. positive (0.44% to 1.5%)	Twenty-four months	Higher long-term positive influence if: 1) the firms is listed in U.S., and 2) the firm adopts a government-advocated sophisticated ITC.	Early ITC adopter,

* Following the practice of leading SLRs of financial event-studies, whenever a particular study reports statistical insignificance (positive or negative) of the abnormal returns, the percentage values (%) are not reported. That is, whenever a percentage or range of percentage is shown in the results column, the corresponding results are statistically significant. Likewise, we have not reported the event windows and tests of significance for studies in which insignificant results were obtained.

References for Online Appendix

Abhishta A, Joosten RA, Nieuwenhuis LJM (2017) Analysing the impact of a DDoS attack announcement on victim stock prices. In: *25th Euromicro International Conference on Parallel, Distributed and Network-based Processing, PDP 2017*, IEEE, St.Petersburg, Russia:354-362.

Acquisti A, Friedman A, Telang RJIP (2006) Is there a cost to privacy breaches? An event study. In: *27th International Conference on Information Systems*, Milwaukee.

Andoh-Baidoo FK, Amoako-Gyampah K, Osei-Bryson KM (2010) How internet security breaches harm market value? *IEEE Security and Privacy* 8(1):36-42.

Arcuri MC, Brogi M, Gandolfi G (2014) The effect of information security breaches on stock returns: Is the cyber crime a threat to firms? In: *European Financial Management Meeting*, Citeseer, Italy 1-12.

Arcuri MC, Brogi M, Gandolfi G (2017) How does cyber crime affect firms? The effect of information security breaches on stock returns. In: *First Italian Conference on Cybersecurity*, Venice, Italy:175-193.

Aytes K, Byers S, Santhanakrishnan M (2006) The economic impact of information security breaches: Firm value and intra-industry effects. In: *12th Americas Conference on Information Systems* Acapulco, Mexico:3293-3300.

Bolster P, Pantalone CH, Trahan EA (2010) Security breaches and firm value. *Journal of Business Valuation and Economic Loss Analysis* 5(1):1-13.

Bose I, Leung ACM (2008) Assessment of phishing announcements on market value of firms. In: *11th International Conference on Information Technology*, Conf. Inf. Technol. ICIT 2008, Bhubaneswar, India:304-307.

Bose I, Leung ACM (2013) The impact of adoption of identity theft countermeasures on firm value. *Decision Support Systems* 55(3):753-763.

Bose I, Leung ACM (2014) Do phishing alerts impact global corporations? A firm value analysis. *Decision Support Systems.* 64(August):67-78.

Bose I, Leung ACM (2019) Adoption of identity theft countermeasures and its short and long-term impact on firm value. *MIS Quarterly* 43(1):313-327.

Campbell K, Gordon LA, Loeb MP, Zhou L (2003) The economic cost of publicly announced information security breaches: Empirical evidence from the stock market. *Journal of Computer Security* 11(3):431-448.

Cardenas J, Nicholas-Donald A, Coronado AS, Parra F, Mahmood MA (2012) The economic impact of security breaches on publicly traded corporations: An empirical investigation. In: *18th Americas Conference on Information Systems*, SEA, US:1393-1400.

Cavusoglu H, Mishra B, Raghunathan S (2004) The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. *International Journal of Electronic Commerce* 9(1):70-104.

Chai S, Kim M, Rao HR (2011) Firms' information security investment decisions: Stock market evidence of investors' behavior. *Decision Support Systems* 50(4, March):651-661.

Chen JV, Li H-C, Yen DC, Bata KV (2012) Did IT consulting firms gain when their clients were breached? *Computers in Human Behavior* 28(2):456-464.

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

Chen Y, Dong F, Chen H, Xu L (2016) Can cross-listing mitigate the impact of an information security breach announcement on a firm's values? In: *7th International Scientific Practical Conference" Innovative Technologies in Engineering".* Yurga, Russia.

Corbet S, Gurdgiev C (2019) What the hack: Systematic risk contagion from cyber events. *International Review of Financial Analysis* 65(October):1-18.

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.

Deane JK, Goldberg DM, Rakes TR, Rees LP (2019) The effect of information security certification announcements on the market value of the firm. *Information Technology and Management* 20(3):107-121.
Ettredge ML, Richardson VJ (2003) Information transfer among internet firms: The case of hacker attacks. *Journal of Information Systems* 17(2):71-82.
Garg A, Curtis J, Halper H (2003) The financial impact of IT security breaches: What do investors think? *Information Systems Security* 12(1):22-33.
Gatzlaff KM, McCullough KA (2010) The effect of data breaches on shareholder wealth. *Risk Management and Insurance Review* 13(1):61-83.
Goel S, Shawky HA (2009) Estimating the market impact of security breach announcements on firm values. *Information & Management* 46(7, October):404-410.
Goel S, Shawky HA (2014) The impact of federal and state notification laws on security breach announcements. *Communications of the Association for Information Systems* 34(1):37-50.
Gordon LA, Loeb MP, Sohail T (2010) Market value of voluntary disclosures concerning information security. *MIS Quarterly* 34(3):567-594.
Gordon LA, Loeb MP, Zhou L (2011) The impact of information security breaches: Has there been a downward shift in costs? *Journal of Computer Security* 19(1):33-56.
Gwebu KL, Wang J, Xie W (2014) Understanding the cost associated with data security breaches. In: *Pacific Asia Conference on Information Systems (PACIS)*, Chengdu, China:386-397.
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, April):337-347.
Hovav A, D'Arcy J (2003) The impact of denial-of-service attack announcements on the market value of firms. *Risk Managment and Insurance Review* 6(2):97-121.
Hovav A, D'Arcy J (2004) The impact of virus attack announcements on the market value of firms. *Information Systems Security* 13(3):32-40.
Hovav A, D'Arcy J (2005) Capital market reaction to defective IT products: The case of computer viruses. *Computers & Security* 24(August):409-424.
Hovav A, Gray P (2014) The ripple effect of an information security breach event: A stakeholder analysis. *Communications of the Association for Information Systems* 34(February):893-912.
Hovav A, Han JY, Kim J (2017) Market reaction to security breach announcements: Evidence from South Korea. *Data Base for Advances in Information Systems* 48(1):11-52.
Hsu C, Wang T, Lu A (2016) The impact of ISO 27001 certification on firm performance. In: *49th Hawaii International Conference on System Sciences (HICSS)*, IEEE, Koloa, HI, US:4842-4848.
Janze C (2017) Intruder alert? How stock markets react to potential IT secuirty breachs: The case of openSSL heartbleed. In: *30th BLED Econference: Digital Transformation-from Connecting Things to Transforming Our Lives* Bled EConference p. 33, Bled Slovenia:245-264.
Jeong CY, Lee SYT, Lim JH (2019) Information security breaches and IT security investments: Impacts on competitors. *Information & Management* 56(5, July):681-695.
Johnson MS, Kang MJ, Lawson T (2017) Stock price reaction to data breaches. *The Journal of Finance Issues* 16(2):1-12.
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.
Khansa L, Cook DF, James T, Bruyaka O (2012) Impact of HIPAA provisions on the stock market value of healthcare institutions, and information security and other information technology firms. *Computers & Security.* 31(6, September):750-770.
Khansa L, Liginlal D (2011) Predicting stock market returns from malicious attacks: A comparative analysis of vector autoregression and time-delayed neural networks. *Decision Support Systems* 51(4):745-759.
Kim JY (2013) Analyzing effects on firms' market value of personal information security breaches. *Journal of Society for e-Business Studies* 18(1):1-12.

Kwon J, Johnson ME (2014) Proactive versus reactive security investments in the healthcare sector. *MIS Quarterly* 38(2):451-471.
Kwon J, Johnson ME (2015) Protecting patient data-the economic perspective of healthcare security. *IEEE Security & Privacy* 13(5):90-95.
Kwon Y-o, Kim B-D (2007) The effect of information security breach and security investment announcement on the market value of Korean firms. *Information Systems Review* 9(1):105-120.
Liginlal D, Sim I, Khansa L (2009) How significant is human error as a cause of privacy breaches? An empirical study and a framework for error management. *Computers & Securty* 28(3, May):215-228.
Malhotra A, Kubowicz Malhotra C (2011) Evaluating customer information breaches as service failures: An event study approach. *Journal of Service Research* 14(1):44-59.
Martin KD, Borah A, Palmatier RW (2017) Data privacy: Effects on customer and firm performance. *Journal of Marketing* 81(1):36-58.
Masaki Ishiguro HT, Kanta Matsuura (2006) The effect of information security incidents on corporate values in the Japanese stock market. In: *International Workshop on the Economics of Securing the Information Infrastructure* 1-15.
Modi SB, Wiles MA, Mishra S (2015) Shareholder value implications of service failures in triads: The case of customer information security breaches. *Journal of Operations Management* 35(May):21-39.
Morse EA, Raval V, Wingender JR (2011) Market price effects of data security breaches: A global perspective. *Information Security Journal* 20(6):263-273.
Muntermann J, Roßnagel H (2009) On the effectiveness of privacy breach disclosure legislation in Europe: Empirical evidence from the US stock market. In: *Nordic Conference on Secure IT Systems*, Springer, Oslo, Norway:1-14.
Nofer M, Hinz O, Muntermann J, Roßnagel H (2014) The economic impact of privacy violations and security breaches. *Businees & Information Systems Engineering* 6(6):339-348.
Patel N (2010) The effect of IT hack announcements on the market value of publicly traded corporations. *Thesis, Duke University*25.
Patsakis C, Charemis A, Papageorgiou A, Mermigas D, Pirounias S (2018) The market's response toward privacy and mass surveillance: The snowden aftermath. *Computers & Security* 73(March):194-206.
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, November):257-271.
Richardson VJ, Smith RE, Watson MW (2019) Much ado about nothing: The (lack of) economic impact of data privacy breaches. *Journal of Information Systems* 33(3):227-265.
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(January):146-154.
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(September):458-469.
Schatz D, Bashroush R (2016) The impact of repeated data breach events on organisations' market value. *Information & Computer Security* 24(1):73-92.
Sinanaj G, Muntermann J (2013) Assessing corporate reputational damage of data breaches: An empirical analysis. In: *26th Bled EConference - EInnovations Challenges and Impacts for Individuals, Organizations and Society*, Bled, Slovenia:78-89.
Sinanaj G, Zafar H (2016) Who wins in a data breach? A comparative study on the intangible costs of data breach incidents. In: *Pacific Asia Conference on Information Systems (PACIS)*, Chiayi City, Taiwan:60-75.
Smith KT, Smith LM, Smith JL (2011) Case studies of cybercrime and their impact on marketing activity and shareholder value. *Academy of Marketing Studies Journal* 15(2):67-82.

Szubartowicz E, Schryen G (2020) Timing in information security: An event study on the impact of information security investment announcements. *Journal of Information System Security* 16(1):3-31.
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.
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.
Wang T, Kannan KN, Ulmer JR (2013) The association between the disclosure and the realization of information security risk factors. *Information Systems Research* 24(2):201-218.
Yayla AA, 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.