Information Technology and Management (2019) 20:107–121
https://doi.org/10.1007/s10799-018-00297-3

The effect of information security certification announcements on the market value of the firm

Jason K. Deane[1] · **David M. Goldberg**[1] · **Terry R. Rakes**[1] · **Loren P. Rees**[1]

Published online: 1 January 2019

Abstract
Information security management has increasingly been recognized as one of the major business challenges of the last decade. While security research has widely recognized that breaches are detrimental to business value, the other side of the equation has received little attention. The literature on the value impact of proactive financial investments into information security management infrastructure and policy is very limited. Unlike most information technology investments, reinforcements to information security management programs suggest a reduction of a firm's risk of damages in future attacks rather than an improvement in a firm's revenue generation. Furthermore, contemporary information security management represents a process-based shift in a firm's operations. In light of the unique information security risks faced by modern firms, we posit several hypotheses related to the value created from information security management program investments. We then present an empirical examination of the effects of information security management program investments on shareholder value. We use a firm's successful completion of the ISO 27001 certification requirements as evidence of its commitment to developing a robust information security management program. Based on 111 public announcements, we find that the associated abnormal stock market reaction is both positive and statistically significant. We further control for firms' industries, sizes, and dates of certification, and we find that they all affect the mean abnormal returns observed. This study demonstrates the capacity for information security management program investments to generate value for firms and further offers guidance for practitioners seeking to maximize shareholder value.

Keywords Information security · Event study · Security investments · Cybersecurity · ISO 27001

1 Introduction

Information security has become a focal point for many organizations. Firms have continually increased their reliance on data and technology, and, in doing so, have increased their information security risk profile [1, 2]. As a result, operational performance setbacks associated with information security breaches have seemingly made their way into the business news headlines with increased frequency, including major attacks against firms such as Home Depot, Target, Sony, Anthem, eBay, and JC Penney [3]. Highlighting the importance of this issue, the White House has weighed in, with the Obama administration issuing new guidelines urging organizations to do more to protect their information assets and stating that failing to do so presents a national security risk [4]. Many prior researchers and practitioners have explored and discussed how costly and economically devastating such security breaches can be, often resulting in the loss of substantial shareholder value [5–9]. Prior research in Information Technology (IT) value creation has shown that general IT investments have resulted in positive stock market reactions [10, 11]. However, prior research considering the stock market reaction to a proactive investment in a robust preventative information security management program has been limited. Information security management investments include several important considerations that distinguish them from typical IT investments and even general computer security investments. IT investments typically represent proactive improvements to a firm's business processes, such as "innovative" investments [10]. These investments may represent the first use of a groundbreaking technology in a firm's industry [10].

✉ David M. Goldberg
goldberg@vt.edu

[1] Department of Business Information Technology, Pamplin College of Business, Virginia Tech, Blacksburg, VA 24061, USA

In comparison, information security management investments involve a much more defensive strengthening of a firm's existing infrastructure. Furthermore, while general IT investments including computer/network security may involve the implementation of a particular product or service, information security management investments have become more process-based in recent years, as information security issues now transcend technical concerns to include information policies and protocols [12]. Chai et al. [13] showed that the stock market values general organizational investments in IT security; their dataset included all companies that had a press release indicating any level of investment in a security implementation. As information security has become more process-based in recent years, however, investments often concern specific security practices and protocols as opposed to purely technical implementations. The ISO 27001 certification specifically focuses on developing a robust Information Security Management System (ISMS), a more holistic and thorough requirement for data management than many other forms of information security investments. By focusing on the ISO 27001 certification, we analyze a uniquely "common size" event, indicating that each firm in our sample has made a comparable investment. In doing so, we provide guidance as to the expected stock market reaction to specific types of information security investments. Furthermore, considering that Chai et al. [13] examine a dataset running from 1997 through 2006, we provide an updated perspective commensurate with the modern state of the market and of the rapidly evolving information security domain. Although this prior work discusses some important considerations such as effects of commercial exploitation, the Sarbanes–Oxley legislation, and choices of security solution vendors [13], we provide coverage of a unique set of hypotheses, including industry, firm size, and recent temporal effects not modeled in prior work. Given the extreme resource commitment that is commonly associated with the development of such a robust information security program, our work will fill an important gap in the literature and help executives determine if such an investment is appropriate for their organizations. We hypothesize that an organization's commitment to the development of a robust information security program represents considerable value to the firm even though it may not directly impact the organization's ability to generate revenue. According to the widely accepted efficient market hypothesis [14], this value should be recognized by the market through the stock price movement. In this work, we test this hypothesis by analyzing the impact on shareholder value of an organization's commitment to developing a robust information security posture.

Specifically, we use the event study methodology to assess the stock market's reaction to ISO/IEC 27001 (often shortened to ISO 27001) certification announcements. The ISO 27001 is recognized worldwide as one of the most thorough and robust information security certifications available [15–17]. The certification is awarded to firms implementing low-risk information security management policies and iteratively testing, developing, and improving their information security infrastructure [15–17]. As such, we use announcements of these certifications to examine our central hypothesis on the value creation power of proactive information security management program investments.

We note that the stock market's reaction to the public announcement of an organization's achievement of such a well-respected certification represents a lower bound on the actual impact of the investment on the overall market value to the firm. As a result of information leakage, some investors may already be aware of the organization's effort to improve their information security posture and thus may have already altered their financial position based on their perception of the likely effectiveness of the program. Hendricks and Singhal [18] noted this same market behavior in relation to announcements of quality awards. After achieving an ISO 27001 certification, it is likely that investors will conduct a reassessment of the probability of the success of such a program. While some of the value of the development of a sound information security management program would have been reflected in stock price movement predating the announcement of the certification, the announcement itself should represent an upward reassessment of the firm's value. Therefore, the stock market reaction that can be attributed solely to the announcement of the certification only represents the lower bound of the actual market value that is associated with the development of a robust information security program.

The remainder of this paper is structured in the following manner. In Sect. 2, we review recent works on information security and IT value creation, and we propose and justify research hypotheses in accordance with the literature in this area. In Sect. 3, we describe our data collection process and provide descriptive statistics on our dataset. Section 4 describes the event study methodology and our application of this methodology to evaluate the market's perception of commitments to information security investments. Next, we describe the results of our analysis and the implications thereof in Sect. 5. Finally, in Sect. 6 we discuss the contributions made to the body of knowledge in this area and recommend several future research directions.

2 Literature review and research hypotheses

Information security breaches arise from a multitude of vectors, such as computer viruses, crimeware, denial of service attacks, insider misuse, and physical theft [19]. Much empirical research on information security describes

the nature of attacks, including the number of attacks that occur and the severity of those attacks [20], often measured in terms of the number of records lost in the breach [19]. Some avenues of research compare the trade-offs associated with different risk management approaches, including risk pooling arrangements [21], law enforcement deterrence [22], recovery countermeasures [23], and reactive versus proactive strategies [24]. Furthermore, a wealth of survey research has been performed to assess the manners in which organizations manage their information security protocols and perceive potential information security threats [25–28]. Several works have sought to assess the impact of information security breaches on an organization, with multiple event studies performed to analyze the economic impact of security breaches under various scenarios [5–9].

Recent research notes that information security breaches have substantially negative effects upon organizations for various reasons. First, breached firms regularly find that potential customers choose to buy from their rivals after being deterred by the prospect of their personal information being compromised [29]. As a result, empirical research finds that firms experiencing security breaches suffer a decrease in stock price on average in the short-term [5–7] and long-term [8, 9]. Second, security breaches may damage a firm's competitive position if company secrets are stolen as part of the security breach. For example, electronics manufacturer HTC experienced a security breach in 2013 by which its confidential design technology was sold to competitors, essentially weakening its ability to differentiate its products in the electronics industry [30]. Third, firms may incur legal liabilities as a result of security breaches; particularly, in the event that firms' customer records are compromised in security breaches, these firms may be subjected to class-action lawsuits from customers. For example, following a breach of consumer financial information, Target was the subject of multiple class action lawsuits in 2013 [31]. Fourth, information security breaches impose organizational costs because firms expend considerable efforts in understanding the nature of the breach and in mending their security protocols to prevent against the breach recurring [5].

Though extant research commonly references the consequences of security breaches for firms, comparatively few articles discuss the impacts of proactive information security measures [32, 33]. Gordon and Loeb present a model for assessing the value of prospective information security investments [34], but empirical evidence on the actual returns of such investments is limited. It follows intuitively that, to the extent that proactive information security measures protect against future security breaches, they also differentiate a firm from competitors as the firm's risk of experiencing the negative effects of a breach decreases. Agrawal et al. [35] note the need for further study on the efficacy of information security standards as a specific type of information security investment. The value creation of general IT investments is well grounded in the literature; however, research in information security investments has only gained traction recently [36]. In addition, it is acknowledged by Wang et al. [36] that several models have been proposed to assist organizations in their determination of how much to invest in information security; however, we are not aware of any works other than the work by Chai et al. [13] that have attempted to confirm and quantify the value creation of such investments. Additionally, prior research by Dos Santos et al. [10] and Im et al. [11] has shown that investments in general Information Technologies result in positive abnormal returns for some firms, and investments in "innovative" IT have particularly substantial value. Unfortunately, it is not clear from the literature where significant investments in the development of a robust information security management system fall in this analysis. As is discussed further below, since investments in information security management programs represent a different type of value proposition for firms than other common IT investments, research on the efficacy of these investments is crucial for both academia and industry.

Broadbent [37, p. 6] defines information technology as "a firm's total investment in computing and communications technology." This category includes investments in hardware, software, telecommunications, and data storage [37]. In contrast, information security is a more specific domain. Von Solms and Van Niekerk [12] define information security as "the preservation of the confidentiality, integrity, and availability of information," a set of criteria that has become known as the CIA triangle. Whitman and Mattord [38] argue that, as firms have had to adapt security protocols to modern challenges, the additional considerations of accuracy, authenticity, utility, and possession necessitate consideration.

We note two important distinctions between typical IT investments and information security management program development investments. First, while most forms of IT investments involve proactive changes to improve a firm's profit impacting business processes [10, 11], information security management programs represent a uniquely defensive posture. These investments do not typically provide firms with a mechanism to perform business processes more efficiently or to improve sales. As such, many managers question if investments in such programs are worthwhile, as returns on such investments do not seem tangible [39, 40]. Indeed, the value of many IT investments is grounded in the fact that the investments are seen as a firm's commitment to cutting-edge technologies to improve its business processes [35]. As innovative investments may allow a firm to secure a competitive advantage by performing at a higher level relative to competitors, Dos Santos et al. [10] found that the market places additional value upon news of these investments. As stakeholders may not view information security

management program investments as yielding this type of advantage, they may question the value of proactive investments in such programs. Second, while many general IT investments involve the technical issues of implementing a particular product or service, information security management program development investments alternatively represent process-based changes in a firm's behavior. While information security investments were previously viewed as technical challenges of implementing superior protocols, the evolution of computers and networks has resulted in an evolution of information security concerns [41]. For example, information security now involves the implementation of protocols for employee handling of information assets [41], a consideration that modern security standards now require [15–17]. As a result of these recent changes in the landscape of information security investments, further study is needed to evaluate their efficacy, representing a significant gap in the literature.

While several standards, certifications, audits and training programs such as NIST, COBIT, BS 7799, ITIL, and PCI DSS, are designed to assist in the development and verification of organizational information security programs, we chose to focus on the ISO/IEC 27001 certification. The ISO/IEC 27001 certification is a robust and internationally accepted information security certification administered by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), which built upon and largely replaced the earlier BS 7799 certification. The certification is awarded subject to the condition that the applicant firm implements, operates, and maintains a highly functioning Information Security Management System (ISMS) in accordance with organizational risk assessment and management objectives [15, 16]. Susanto et al. [17] offer further justification for this standard's characteristics, concluding that the ISO 27001 offers superior usability relative to other major standards and that it is better recognized by stakeholders [17]. We chose to focus on this certification alone for a number of reasons. First, the ISO umbrella of standards is recognized worldwide for its breadth and quality. Some standards, such as PCI DSS, refer to only very specific aspects of a firm's information security efforts, such as handling of credit card transactions. Others, such as COBIT or ITIL, are focused on IT service management and IT governance, which consider the alignment of a firm's IT services and its business objectives, of which information security is one of several areas of focus. NIST is recognized as a vital standard for the handling of federal data, but it is a standard for data management practices rather than a certification that firms achieve. The ISO/IEC 27001 certification is widely accepted as the international benchmark for ISMS [17] and is arguably the most robust and expensive of security standards to achieve and is projected to soon become the domestic de facto standard [16], leaving many organizations trying to determine if it is worth the substantial investment. It is widely acknowledged that achieving the ISO/IEC 27001 certification can be a very grueling time and resource intensive process, but it sends a clear message with respect to an organization's commitment to information security. The cost of an ISO 270001 certification averages about $100,000 [42], although this figure represents a lower bound for larger publicly traded firms. Costs associated with the certification increase for larger organizations and for organizations with larger gaps between present implementations and ISO 27001-compliant solutions. Second, this information security certification represents a uniquely "common size" event, as each firm that earns this certification has attained a similar level of security competency. While it may be difficult to reconcile differences between the diverse set of security programs, this certification indicates notable similarity in firms' achievements. As a firm's efforts to earn this certification are indicative of substantial information security infrastructure investment and management, which protects against future attacks, we expect that the stock market will view firms having achieved the ISO 27001 certification as less risky and, therefore, more valuable relative to competitors. As such, we posit Hypothesis 1:

H1: ISO 27001 certification announcements are associated with positive abnormal market value creation.

2.1 Industry effect

Im et al. [11] 's seminal work on IT value creation controlled for industry type by separating their dataset into financial and manufacturing firms. Their cross-group comparison found that more modern IT investments by financial firms generated superior value in comparison to that created for manufacturing firms. We, however, do not anticipate that findings are generalizable when focusing on the value of targeted IT investments in information security. As mentioned previously, earning the ISO 27001 certification may be seen by the market as a preventative measure protecting against exceedingly costly future security attacks; as such, we expect the market to place the highest value on ISO 27001 certifications earned by firms from industries in which damaging security attacks have been historically frequent. Earning the information security certification should immediately differentiate a firm in a vulnerable industry from its rivals, providing it a competitive advantage as an information secure firm in an information insecure industry. Utilizing Verizon's Data Breach Investigations Report [19], we identify the industries with the most serious recent history of information security breaches. Verizon's DBIR is based on direct incident data collected by Verizon and 70 other industry partners. While we do not claim that their dataset is all-encompassing, we are confident that it provides a representative sample of the

overall population of information security breaches. Given the reluctance of firms to openly admit that they have experienced an information security breach, Verizon's report does not include company names but does include the general demographic information including the company's industry for this set of breaches. Of the 2122 confirmed data loss events in Verizon's sample, the financial services and manufacturing industries were the two private-sector industries in which the greatest number of data breaches occurred [19].[1] Therefore, we expect information security certifications to be of paramount significance to investors in both of these industries. This notion further differentiates the value of information security investments from general IT investments. Im et al. [11] and Dos Santos et al. [10] both note an expectation that firms in the financial industry should derive greater benefit from general IT investments than firms in the manufacturing industry. Dos Santos et al. [10] specifically note that IT investments ought to be more beneficial to financial firms due to the information-intensive nature of the industry. This assertion is further supported by evidence that banks are able to use nuanced information processing to improve their performance [43]. However, as information security more specifically concerns prevention of data breaches as opposed to enhancing a firm's revenue generation, we expect that firms most targeted by attacks have the most to gain from an information security certification, so both financial and manufacturing firms should benefit from information security certifications. Based on this premise, we posit Hypothesis 2A and Hypothesis 2B:

H2A: Financial services firms' ISO 27001 certification announcements are associated with greater than average positive abnormal market returns.

H2B: Manufacturing firms' ISO 27001 certification announcements are associated with greater than average positive abnormal market returns.

2.2 Firm size effect

Additionally, we expect the market to react differently to the news of an ISO 27001 certification depending upon the firm's size. Im et al. [11] hypothesized that IT investments would result in a greater impact to market value for smaller firms, and their findings supported this hypothesis. We also expect that the market will react more positively to information security certification announcements from small firms than to certification announcements from large firms. We present two justifications for this hypothesis. First, we expect small firms to run more narrowly concentrated operations, and, as such, these firms may require a spotless operating record in order to remain profitable. By contrast, while an information security breach is certainly damaging for a larger firm, we expect that these firms will run broader operations allowing for unaffected business units to financially absorb the impact of a security breach in other units. As such, we expect that receiving an information security certification should greatly alleviate concerns about a security breach adversely affecting the health of a small firm's main business unit. Second, as Hendricks and Singhal [18] note, larger firms tend to receive closer attention than smaller firms, and, as such, the market may have access to more public information about larger firms than about smaller firms. Particularly in the case of an ISO 27001 certification, the process of improving information security standards may occur over several months, during which investors may revise their expectations of the firm if given access to new information. In accordance with the efficient market hypothesis, we expect the market to react to new information about a firm immediately and for that information to be reflected in a change in stock price. Therefore, because some investors may already have altered their valuation of a firm during the period preceding the issue of the certification due to knowledge of that firm's commitment to the development of a robust information security management program, we expect that the market will find news of an ISO 27001 certification to be less surprising for a larger firm than for a smaller firm. The notion that smaller firms' actions are more difficult for the market to anticipate is empirically verified by Brown et al. [44], who find that the market reacts with greater magnitude to earnings announcements of small firms than to earnings announcements of large firms. Of course, this rationale is not an argument that it is less important for larger firms to invest in information security management programs, but rather that the market's reaction to a larger firm's investment in an information security management program should result in a less striking abnormal return during the announcement's event window due to the firm's characteristics and the efficient market hypothesis. As such, we posit Hypothesis 3:

H3: Smaller firms' ISO 27001 certification announcements are associated with greater positive abnormal market returns than larger firms' ISO 27001 certification announcements.

[1] According to Verizon's Data Breach Investigations Report, the public or government industry actually included the greatest number of confirmed data breaches with 303, although these entities are outside the scope of the event study methodology, which focuses on publicly traded firms. The financial services industry included 277 confirmed data breaches, followed by 235 breaches in the manufacturing industry, 223 breaches in the accommodations industry, and 164 breaches in the retail industry.

2.3 Time lag effect

Finally, given that the threat domain for information security has progressed throughout the duration of our study period, we expect the market's reactions to information concerning new ISO 27001 certifications to have adapted in response to that progression. A major chapter in information security began in 2013, which is colloquially referred to as "the year of the mega breach" [45]. Relative to 2012, total data breaches increased by 62%, and targeted attack campaigns increased by 92% [45, 46]. In addition, eight different breaches each resulted in exposure of ten million or more identities compared to only one breach of that magnitude in 2012; in total, 2013s breaches exposed over 552 million identities [45]. Several major breaches, including the Target breach, were widely-publicized, making consumers aware of the possibility that their information could be compromised and altering their buying behavior; following Target's breach, its earnings fell 46% in the fourth quarter of 2013 [31, 47]. Possibly in response to the changing risk environment, 2013 also marked the year in which the greatest number of firms from our sample received ISO 27001 certifications (see Panel C of Table 2). Consequently, we expect perceived value of information security certifications to have become more apparent to the market since 2013, and we posit Hypothesis 4:

H4: ISO 27001 certification announcements since 2013 are associated with greater positive abnormal share price reactions than ISO 27001 certification announcements before 2013.

3 Sample selection procedure and data description

The results of this paper are based on a sample of public announcements stating that a firm had achieved the ISO 27001 certification. The search covered the time period from 2005 through 2015. In particular, because we are interested in the market's reaction to an announcement of a recently earned ISO 27001 certification, we concentrated our search on articles containing keywords that referenced a newly earned certification rather than articles that referenced a pre-existing certification. Key words used in the search are listed in Panel A of Table 1. In Panel B of Table 1, we detail the search sources used to find certification announcements.

Unfortunately, not all of the announcements that were discovered were useable. Several had to be filtered out of our dataset based on the criteria listed below.

- Announcements of ISO 27001 certifications that pertained to firms that were not publicly traded.

Table 1 Keywords and search sources employed in the search for ISO 27001 announcements

Panel A: Keywords employed in the search for ISO 27001 announcements	
ISO27001, ISO 27001, ISO/IEC 27001, ISO27001 certification, ISO 27001 certification, ISO/IEC 27001 certification, ISO27001 certified, ISO 27001 certified, ISO/IEC 27001 certified, IS certification, IT certification, IT security certification, security certification, information security certification, ISO security certification, ISO/IEC security certification	
Accomplish, accomplished, accomplishes, accomplishment, announce, announced, announcement, announces, award, awarded, awards, became, becomes, becoming, earned, earns, qualification, qualified, qualifies, qualify, recognition, recognize, recognized, recognizes	
Panel B: Search sources	
BSI Group Database	PR Newswire
Yahoo! Finance	PR Web
Bloomberg	Reuters
	Business Wire
	Market Wired

Table 2 Description of the sample of 111 announcements of ISO 27001 certifications

Measure[a]	Mean	Median	SD	Maximum	Minimum
Panel A: Descriptive statistics of firm financial characteristics					
Market capitalization	36,551	6858	69,622	359,848	13
Total assets	42,013	3113	92,425	520,701	4
Sales	18,661	2344	32,555	128,752	4
Net income	1594	153	4345	21,863	− 6082
Stock market			Count		Percentage
Panel B: Descriptive statistics of stock exchange representation					
NYSE			87		78.38
NASDAQ			24		21.62
All stock exchanges			111		100.00
Prior breach			Count		Percentage
Panel C: Descriptive statistics on prior breach status					
Yes			31		27.93
No			80		72.07
All firms			111		100.00
Year			Count		Percentage
Panel D: Distribution of announcement years					
2005			2		1.80
2006			1		0.90
2007			5		4.50
2008			11		9.91
2009			2		1.80
2010			10		9.01
2011			14		12.61
2012			13		11.71
2013			28		25.23
2014			15		13.51
2015			10		9.01
2005–2015			111		100.00
Description	Count		Percentage		SIC code range
Panel E: Descriptive statistics of industry representation					
Manufacturing	24		21.62		2000–3999
Communications	11		9.91		4812–4899
Financial services	14		12.61		6000–6799
Computer software/services	51		45.95		7370–7377
Other[b]	11		9.91		Various
All industries	111		100.00		

[a]All measures are reported in millions of US dollars

[b]"Other" contains 6 unique industry classifications, and each classification contains no more than 4 members

- Announcements of ISO 27001 certifications that pertained to firms lacking sufficient stock price information at the time of the announcement in the Center for Research in Security Prices (CRSP) dataset, which includes stocks traded on the New York Stock Exchange (NYSE) or NASDAQ. We also removed announcements for which we could not collect stock price data for an estimation period of at least 40 days, which we discuss further in Sect. 4.
- Announcements of the same ISO 27001 certifications that were found from multiple data sources. In this case, we stored the article with the earliest date of publication

and removed all other articles referencing the same certification.

A thorough search of the above sources revealed 124 useable announcements. Using this initial sample, we performed an additional news search on each firm to identify any possible confounding events, or events outside the event type being studied that may have affected abnormal returns within the event window [48]. A confounding event is any event that confuses the results. In our situation, this would be an event related to the company in question that could have impacted the abnormal return recognized during the trading window utilized for the study. For example, one firm in our sample was involved in a major court case for which announcements were released during the same three-day period that comprised the event window for the ISO 27001 certification announcement; as such, the market's reaction to the legal proceedings could easily have obscured the market's reaction to the new certification announcement. Therefore, this company and any others that had similar events were removed. Our analysis revealed 13 such confounding events, resulting in a final dataset of 111 useable firms.

In addition to the date of the announcement, as part of the data collection process we identified basic financial characteristics of each firm and grouped firms into industries by SIC (Standard Industrial Classification) codes. We provide descriptive statistics on financial characteristics of our sample in Panel A of Table 2, descriptive statistics on the stock markets represented in our sample in Panel B of Table 2, descriptive statistics on prior breach statuses represented in our sample in Panel C of Table 2, the distribution of announcement years in our sample in Panel D of Table 2, and descriptive statistics on industries represented in our sample in Panel E of Table 2. Descriptive statistics on firm financial characteristics and industry representation were obtained from S&P Global's COMPUSTAT database, which contains financial data on major firms around the world. Firms' histories of breaches were obtained from the Privacy Rights Clearinghouse data breach database, which contains detailed data on data breaches since 2005.

4 Methodology

4.1 Parametric analysis

We employ the event study methodology in order to quantify the estimated change in shareholder value associated with ISO 27001 certification announcements. The event study methodology is a well-accepted approach used to estimate the market's response to specific events that affect shareholder value for given firms while accounting for stimuli affecting the entire market [49, 50]. While initially pioneered in the finance domain, the event study methodology has gained widespread acceptance and usage in the information systems domain in recent years [51–58]. In event study literature, the phrase "abnormal returns" is used to refer to estimates of the magnitude and direction at which a change in stock price can be associated with a specific event of study as opposed to the broader flux and flow of the entire stock market. An important theoretical foundation for the event study methodology is the premise that, given an efficient market, the impact of new information about a firm (i.e., an event) is immediately met with a corresponding adjustment in that firm's stock price. As the market gathers new information, investors revise their expectations for the firm, and their valuation of the firm, reflected in that firm's stock price, changes accordingly. As a result, by observing the manner in which stock prices react in short time periods around events, we may understand and approximate the impact that the event has had upon those stock prices, which is the difference between a firm's actual returns as influenced by an event and its expected returns in absence of the event. In this section, we describe the key features underpinning the event study techniques and detail our methodology for the estimation of these abnormal returns.

Various models have been employed for the estimation of abnormal returns; we apply the market model, a derivation of the commonly accepted Capital Asset Pricing Model (CAPM), in this event study. Brown and Warner's analysis finds the market model to be well specified [49, 50]; furthermore, Armitage found in comparing various event study models via simulation experiments that the market model outperforms its competitors and that standardizing abnormal returns and using a t test is typically the best test of significance when using the market model [59]. Like the CAPM, the market model suggests a linear relationship between a stock's return and the return on a portfolio consisting of all stocks comprising the market (hereafter referred to as market return):

$$r_{it} = \alpha_i + \beta_i r_{mt} + \varepsilon_{it} \tag{1}$$

Given a stock i, r_{it} represents the return of that stock on day t. Next, α_i represents the y-intercept of the linear relationship between stock i and the market return, essentially signifying a constant daily return for stock i. β_i represents the slope of the linear relationship between stock i and the market return, and r_{mt} represents the market return on day t. As such, the multiplication of these two terms in $\beta_i r_{mt}$ represents the portion of a stock's return that is explained by movements in the entire market, m, rather than stock i alone. Therefore, across different stocks, the magnitude and direction of β_i represent the expected impact of market movements upon the given firm's stock return. Finally, ε_{it} represents error for stock i on day t, or the portion of the stock's movement on day t that cannot be explained by market movements and instead encapsulates the impacts of stock i's movements in response to new information about the specific firm.

As is widely accepted in event study analysis, the model parameters in (1) are determined using an Ordinary Least Squares (OLS) regression for each firm i by analyzing actual stock price for that firm over an estimation period of 255 trading days, where available. We required that each firm had useable data for at least 40 days, and any announcements for which this data was unavailable were removed from our event study. Furthermore, we estimated market returns for construction of the OLS models using an equally weighted index containing securities included in the CRSP dataset, including the NYSE and NASDAQ. As a product of this regression analysis, we estimated values for $\hat{\alpha}_i$, $\hat{\beta}_i$, and $\hat{S}^2_{\varepsilon_i}$. The following expression equates the abnormal return for firm i on day t, written as A_{it}, to the difference between r_{it}, which represents the observed return for firm i on day t, and $\hat{\alpha}_i + \hat{\beta}_i r_{mt}$, which represents the expected return for firm i on day t:

$$A_{it} = r_{it} - \left(\hat{\alpha}_i + \hat{\beta}_i r_{mt}\right) = r_{it} - \hat{\alpha}_i - \hat{\beta}_i r_{mt} \tag{2}$$

We define N as the total number of firms, i, included in our sample. We calculate the daily mean abnormal return on day t, written as $\bar{A}_t$, in the following:

$$\bar{A}_t = \sum_{i=1}^{N} \frac{A_{it}}{N} \tag{3}$$

We analyze the abnormal return over a window of two days. The generalized formula for the cumulative abnormal return over a period of days, $t_1, \ldots, t_f$, is defined in the following expression as the sum of the estimated daily mean abnormal returns on each day t, $\bar{A}_t$:

$$CAR\left(t_1, t_f\right) = \sum_{t=t_1}^{t=t_f} \bar{A}_t \tag{4}$$

Furthermore, in order to test the significance of firm i's estimated abnormal return, we calculate the standardized abnormal return, A^s_{it}, by dividing firm i's abnormal return, A_{it}, by its estimated standard deviation, $\hat{S}_{\varepsilon_i}$.

$$A^s_{it} = \frac{A_{it}}{\hat{S}_{\varepsilon_i}} \tag{5}$$

Next, utilizing this standardized abnormal return, we calculate a test statistic, T_t, in (6). Our use of this technique posits a null hypothesis for abnormal returns under which the expected mean abnormal return is 0 with a variance of $\hat{S}^2_{\varepsilon_i}$. Based on the Central Limit Theorem, the sum of N standardized abnormal returns is distributed normally about a mean of 0 with a variance of N:

$$T_t = \sum_{i=1}^{N} \frac{A^s_{it}}{\sqrt{N}} \tag{6}$$

Finally, we present the equation for evaluating multiple days, $t_1, \ldots, t_f$, of abnormal returns. Given that each firm's returns follow like (i.e., normal) distributions and that each firm's abnormal returns are independent of each other firm's abnormal returns, the multiple day test statistic, T_c, is expressed as:

$$T_c = \sum_{i=1}^{N} \frac{\left(\sum_{t=t_1}^{t=t_f} A_{it}\right) / \sqrt{\sum_{t=t_1}^{t=t_f} \hat{S}^2_{\varepsilon_i}}}{\sqrt{N}} \tag{7}$$

The formulas in this section reflect the market model, which has been studied extensively [49, 50, 60] since the introduction of the event study methodology by Fama et al. [14]. According to Binder [61], this methodology, using formulas similar to the above, is widely accepted for analyzing the impacts of corporate events across diverse study areas. Additionally, the parametric t test is a well-accepted tool for testing statistical significance in an event study framework [59, 62]. The t test is considered to be the best framework for analyzing statistical significance in most event study frameworks and to be relatively robust [59].

For robustness, we supplement the results of the market model with the Fama–French–Carhart model, which suggests a revised estimation procedure for estimating abnormal returns. Fama and French [63] extend the market model's simple linear regression model with a three-factor multiple regression model, which also considers market capitalization values and book-to-market ratios alongside the market return. Carhart [64] offers a further extension of this model by considering a fourth factor, momentum, in addition to these factors. We display results from both estimation procedures to ensure the robustness of our results.

4.2 Event study structure

In the following, we detail the organization of the event study. Figure 1 displays a schematic of our event study timeline. We use a 255-day estimation period to build an OLS regression model for each firm, which is approximately equivalent to one trading year. Where data for 255 days of a firm's activity was unavailable, we required at least 40 days of data availability for a firm to be included in the sample. The estimation period is arranged such that it ends 45 days prior to our event window. Any overlap between the two time periods would cause the regression model to be influenced by the event itself [65], and, as Willi and Knolmayer advise [66], we institute a buffer between the estimation period and

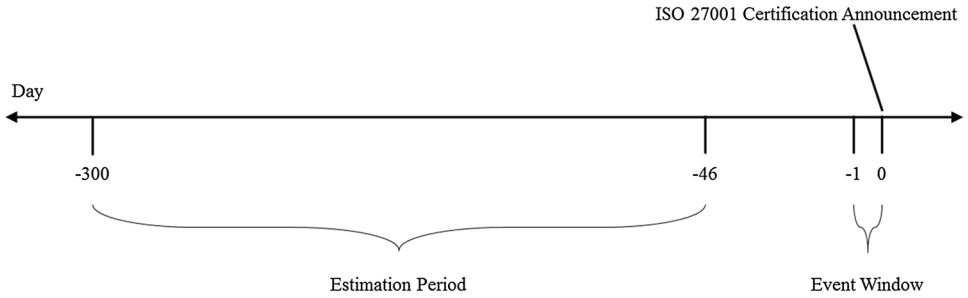

Fig. 1 Structure of the event study timeline

the event window to ensure that no residual effects of either time period "contaminate" the other. We employ a 2-day event window in our event study, an approach commonly employed in information systems event study research [51]. In addition to the day of the ISO 27001 announcement, we include the day before the event in our event window to account for the prospect that information about the firm's certification may have circulated before the date of public announcement. However, we do not include additional days because longer event windows allow for more confounding events to influence the observed abnormal returns. In addition, we expect the market to react to new information about a firm immediately per the efficient market hypothesis, so a 2-day event window should sufficiently capture the market's response [48].

In the event that the announcement of a newly earned certification occurred on a day that the market was closed or that the announcement occurred after the market's trading hours, we treat the next trading day as the event date (day 0). This is a common practice in event study research and verifies that our event date occurs on the first day that the market had an opportunity to react to the announcement [67]. Consistent with event study convention, we term the event date day 0, the trading date immediately following the event date day +1, and trading date immediately preceding the event date day −1, and so on.

5 Empirical results

5.1 Sub-sample analysis

5.1.1 Overall market reaction

In this section, we detail the results of our event study as applied to our research hypotheses. Table 3 contains the data to support our evaluation of Hypothesis 1. We observed that firms experienced positive abnormal returns on both individual days within the event window, day −1 and day 0, with a mean abnormal return of 0.72% over this period. Furthermore, the *t*-statistic was statistically significant on day 0 and for the window encompassing both days. The Fama–French–Carhart model largely corroborated the results of the market model. This supports our notion that the market places significant value upon the organizational commitment to information security, as a firm's efforts to earn the ISO 27001 certification indicate a commitment to information security practices and that the firm has already achieved a highly functioning ISMS.

Given the descriptive financial data presented in Panel A of Table 2, this abnormal return presents an enormous opportunity for managers: as the average firm studied in this paper has a market capitalization of $36.55 billion, an additional return of 0.72% represents an average of a $263.17 million increase in value. Furthermore, as noted previously, due to the potential for information leakage, this figure represents a lower bound for the potential benefits that investing firms may garner [18]. While we expect the event window to encapsulate the market's reaction to a newly earned ISO 27001 certification, we also tested a 20-day time period after our event window (days +1 through +20) to ensure that the observed abnormal return was not an ephemeral increase in valuation. That is, had the market consistently responded with negative abnormal returns in the days following the event window, it may have indicated that the certification only temporarily altered investors' valuations rather than indicating a valuable capability in the long term. We observed a mean abnormal return of 0.07% during this

Table 3 Abnormal returns for the sample of 111 announcements of ISO 27001 certifications

	Day −1	Day 0	Days −1 and 0
Panel A: Full sample of announcements ($N=111$): market model			
Mean abnormal return	0.27%	0.45%	0.72%
Abnormal returns positive (%)	56.76%	58.56%	62.16%
t-statistic	1.53	1.99*	2.51**
Panel B: Full sample of announcements ($N=111$): Fama–French–Carhart model			
Mean abnormal return	0.42%	0.36%	0.78%
Abnormal returns positive (%)	57.66%	62.16%	63.06%
t-statistic	1.77*	1.54	2.34**

The symbols *, **, and *** represent statistical significance at 0.10, 0.05, and 0.01 levels respectively. All tests are two-tailed

Table 4 Abnormal returns grouped by industry classifications

	Day −1	Day 0	Days −1 and 0
Panel A: Announcements in the financial services industry ($N=14$): market model			
Mean abnormal return	0.34%	0.73%	1.07%
Abnormal returns positive (%)	57.14%	64.29%	78.57%
t-statistic	0.61	2.33*	2.26*
Panel B: Announcements in the manufacturing industry ($N=24$): market model			
Mean abnormal return	0.74%	0.38%	1.12%
Abnormal returns positive (%)	83.33%	58.33%	87.50%
t-statistic	2.40**	1.50	3.27***
Panel C: Announcements in the financial services industry ($N=14$): Fama–French–Carhart model			
Mean abnormal return	0.35%	0.70%	1.05%
Abnormal returns positive (%)	57.14%	57.14%	78.57%
t-statistic	0.50	2.35*	2.31*
Panel D: Announcements in the manufacturing industry ($N=24$): Fama–French–Carhart model			
Mean abnormal return	0.76%	0.43%	1.19%
Abnormal returns positive (%)	75.00%	50.00%	91.67%
t-statistic	1.95*	1.21	3.17**

The symbols *, **, and *** represent statistical significance at 0.10, 0.05, and 0.01 levels respectively. All tests are two-tailed

time period, and 53.15% of returns were positive. This mean abnormal return is less than 0.01% per day, or a rather minor change in value. The mean abnormal returns for this period were not significant via our statistical test, indicating that the market's reaction during this time period is more easily attributable to various confounding events than a consistent response to the ISO 27001 certification. As such, we did not observe evidence that the market responds significantly in the period following the ISO 27001 certification announcement; instead, the event window (−1, 0) appears to capture the majority of the changes in shareholder value as a result of the ISO 27001 certification announcement.

5.1.2 Industry type effect

Table 4 contains the data to support our evaluation of Hypothesis 2A and Hypothesis 2B. Utilizing the SIC code groupings outlined in Panel D of Table 2, we repeated our analysis for the firms in each of the industries represented in our sample. Supporting our hypotheses, the mean abnormal returns from the financial services and manufacturing industries were the highest and were much greater than the mean abnormal return from our sample as a whole. The majority of abnormal returns for the financial services industry were positive for each day of the event window, and the mean abnormal return over the 2-day event window of 1.07% outperformed the mean abnormal return of 0.72% observed for the sample as a whole. Abnormal returns on day −1 were not statistically significant via the *t*-statistic, and the statistical tests indicated statistical significance at the 0.10 level for abnormal returns on day 0 and for the event window (−1, 0). Similarly, we also found that the majority of abnormal returns for the manufacturing industry were positive for each day of the event window. The mean abnormal return over the 2-day event window was 1.12% for this industry, also outperforming the average of 0.72% observed for the sample as a whole. Our analysis indicated statistical significance for abnormal returns on each day of the event window and for the window itself. Again, the Fama–Franch–Carhart model did not substantially differ from the market model. In sum, the evidence collected supports our hypotheses, which we base on the notion that firms in industries with histories of frequent breaches, the financial services and manufacturing industries, will realize relatively higher differentiation from a commitment to information security.

Table 5 Abnormal returns grouped by firm size (market capitalization)

	Day −1	Day 0	Days −1 and 0
Panel A: Announcements made by small sized firms ($N=37$): market model			
Mean abnormal return	0.44%	0.81%	1.25%
Abnormal returns positive (%)	54.05%	62.16%	56.76%
t-statistic	0.79	1.45	2.16*
Panel B: Announcements made by medium sized firms ($N=37$): market model			
Mean abnormal return	0.12%	0.33%	0.45%
Abnormal returns positive (%)	59.46%	54.05%	64.86%
t-statistic	0.41	1.86*	1.22
Panel C: Announcements made by large sized firms ($N=37$): market model			
Mean abnormal return	0.21%	0.18%	0.40%
Abnormal returns positive (%)	56.76%	59.46%	62.16%
t-statistic	1.24	0.19	1.08
Panel D: Announcements made by small sized firms ($N=37$): Fama–French–Carhart model			
Mean abnormal return	0.69%	0.61%	1.30%
Abnormal returns positive (%)	56.76%	62.16%	62.16%
t-statistic	1.26	1.12	1.68*
Panel E: Announcements made by medium sized firms ($N=37$): Fama–French–Carhart model			
Mean abnormal return	0.23%	0.32%	0.56%
Abnormal returns positive (%)	56.76%	67.57%	67.17%
t-statistic	0.75	1.03	1.25
Panel F: Announcements made by large sized firms ($N=37$): Fama–French–Carhart model			
Mean abnormal return	0.34%	0.16%	0.49%
Abnormal returns positive (%)	59.46%	56.76%	59.46%
t-statistic	1.11	0.98	1.31

5.1.3 Firm size effect

Table 5 contains the data to support our evaluation of Hypothesis 3. To evaluate our hypotheses that smaller firms experienced greater abnormal returns than larger firms, we grouped our firms into three categories by market capitalization: small, medium, and large. Market capitalization is a common method of measuring firm size in event study research [68]. The evidence we observed largely supported our hypothesis: smaller firms experienced greater positive abnormal returns than larger firms. Our analyses using the *t*-statistic reached the statistical result that small firms' abnormal returns, which totaled 1.25%, were statistically insignificant on day − 1 and day 0 and statistically significant at the 0.10 level over the 2-day window (− 1, 0). Medium firms were associated with a mean abnormal return of 0.45% over the 2-day window. Returns were statistically significant on day 0 but not on day − 1. Over the 2-day window, the observed *t*-statistic was insignificant. Finally, the largest third of firms in our sample experienced the lowest mean abnormal return of 0.40%. In addition, our analysis indicated that each day within the event window had statistically insignificant abnormal returns, and the 2-day window was statistically insignificant. We observed that the mean abnormal return for small firms was more than double the mean abnormal return for medium firms and more than triple the mean abnormal return for large firms. While all three groups experienced positive stock market reactions, small firms greatly outperformed larger firms, supporting our hypothesis. The robustness tests using the Fama–Franch–Carhart model corroborated this finding.

5.1.4 Time lag effect

Table 6 contains the data to support our evaluation of Hypothesis 4. Separating events before 2013 from events on or after the first day of 2013 yielded similarly sized groups of 58 and 53 events, respectively. Our analysis strongly supported our hypothesis that announcements made beginning in 2013 would be associated with greater positive abnormal returns than events before 2013. Although events before 2013 were associated with a positive mean abnormal return of 0.45%, and more than half of these events were associated with positive abnormal returns, the *t*-statistic failed to detect statistical significance on either of the individual days within the event window or the window itself. In contrast, events on or after the first day of 2013 were associated with a greater mean abnormal return of 1.02%, and a greater percentage of abnormal returns were positive for each day of the event window and for the window itself. In addition, we found that both days within the 2-day event window and the event window itself were statistically significant. Again, the results from the Fama–French–Carhart model corroborated the results from the market model. Events since 2013 were associated with more than twice the mean abnormal return of events before 2013, supporting our notion that the market would value these more recent certifications more highly in light of recent changes in the nature of information security risk.

Table 6 Abnormal returns grouped by time period

	Day −1	Day 0	Days −1 and 0
Panel A: Announcements before 2013 ($N=58$): market model			
Mean abnormal return	0.10%	0.35%	0.45%
Abnormal returns positive (%)	51.72%	50.00%	56.90%
t-statistic	0.07	0.49	0.39
Panel B: Announcements since 2013 ($N=53$): market model			
Mean abnormal return	0.45%	0.57%	1.02%
Abnormal returns positive (%)	62.26%	69.81%	69.81%
t-statistic	2.08*	2.70***	3.37***
Panel C: Announcements before 2013 ($N=58$): Fama–French–Carhart model			
Mean abnormal return	0.23%	0.25%	0.48%
Abnormal returns positive (%)	51.72%	56.90%	62.07%
t-statistic	0.45	0.71	0.77
Panel D: Announcements since 2013 ($N=53$): Fama–French–Carhart model			
Mean abnormal return	0.51%	0.49%	1.01%
Abnormal returns positive (%)	64.15%	67.92%	64.15%
t-statistic	1.70*	2.62***	3.34***

The symbols *, **, and *** represent statistical significance at 0.10, 0.05, and 0.01 levels respectively. All tests are two-tailed

5.2 Regression analysis

As a supplement to our sub-sample analysis, we also provide a regression analysis to ensure the robustness of our findings (Table 7). The regression analysis will consider each of the hypotheses jointly to determine whether each hypothesis is supported while controlling for additional effects. In our regression model, we consider variables for each of the hypotheses studied: industry effect, firm size effect, and time lag effect. We considered hypotheses concerning abnormal returns for two specific industries: financial services (H2A) and manufacturing (H2B). For each of these hypotheses, we created a binary variable equal to one if the firm participated in the industry of interest and 0 otherwise. We modeled the firm size effect using market capitalization, and we performed a logarithmic transformation on the market capitalization values to account for the substantial range in firm sizes (see Table 2) [69]. Next, we created a binary variable equal to one if the firm's event date was since 2013 and zero otherwise. Finally, we included a final variable to control for whether each firm had experienced a data breach prior to receiving the certification, which we set equal to 1 if the firm had experienced a prior breach and 0 otherwise. Hence, we construct the regression model in (8).

Table 7 Regression analyses of abnormal returns in the window (−1, 0)

	Coefficient	*t*
Panel A: Regression coefficients and significance tests: market model		
Intercept	1.17	1.03
Financial services	1.12	2.02**
Manufacturing	1.77	2.10**
Log (market capitalization)	− 0.34	− 1.16
Time lag	1.14	2.37**
Prior breach	− 0.48	− 0.78
Panel B: Model metrics: market model		
R^2	0.14	
Adjusted R^2	0.10	
F	3.21***	
Panel C: Regression coefficients and significance tests: Fama–French–Carhart model		
Intercept	1.42	1.36
Financial services	0.90	1.67*
Manufacturing	1.40	2.05**
Log (market capitalization)	− 0.40	− 1.57
Time lag	1.00	2.03**
Prior breach	− 0.27	− 0.60
Panel D: Model metrics: Fama–French–Carhart model		
R^2	0.13	
Adjusted R^2	0.09	
F	2.57**	

Multicollinearity was assessed using variance inflation factors (VIF). Multicollinearity is problematic if any VIF values exceed 10; in both models, all VIF values were less than 2.

*, **, and *** indicate statistical significance at the 0.10, 0.05, and 0.01 levels respectively. All tests are two-tailed

$$CAR = \beta_0 + \beta_1 Financial\ services + \beta_2 Manufacturing + \beta_3 Log(market\ capitalization) + \beta_4 Time\ lag + \beta_5 Prior\ breach + \varepsilon \quad (8)$$

The regression model largely corroborated the results of the sub-sample analysis. Each of the coefficients reflected the same direction of relationship with the dependent variable that we observed in the sub-sample analysis. In the market model regression analysis, there were significant relationships for financial services firms and manufacturing firms at the 0.05 level, indicating the firms in these industries tended to experience greater positive abnormal returns than other firms. We found that market capitalization was inversely related with abnormal returns, indicating that smaller firms experienced greater abnormal returns than larger firms; however, this relationship was not statistically significant in the regression analysis. The time lag hypothesis was supported at the 0.05 level, indicating that firms that had been certified since 2013 experienced greater abnormal returns than firms certified prior to 2013. Finally, we did observe that firms that had experienced a prior breach experienced lesser abnormal returns than firms that had not experienced a prior breach, although this relationship was not statistically significant. When using the Fama–French–Carhart model rather than the market model to estimate abnormal returns, we observed broadly consistent results. In sum, the results from our regression analysis largely corroborated the results of our sub-sample analyses.

6 Research limitations, future research directions, summary and conclusions

Following expansions of information technology infrastructure in the past decade, information security policy has become a vital consideration for managers. Indeed, many firms have experienced the negative consequences associated with security breaches; this study serves to address the value to the stock market of the proactive development of a robust information security management program, and it specifically addresses the extent to which the market perceives these investments as a valuable reduction of information security risk. Using ISO 27001 certifications as evidence that firms have successfully developed such a program; we employ the event study methodology to examine empirically the abnormal returns associated with the announcements of these certifications. We observe positive and statistically significant abnormal returns in the

2-day window comprising the day of and the day preceding these announcements, indicating that the market perceives significant value in commitments to information security risk management. Furthermore, we observe that firms in the historically vulnerable manufacturing and financial services industries derived greater benefit from these certifications, indicating a greater level of differentiation between these firms and their competitors. Also, the observed evidence is consistent with our notion that small firms acquire a slightly greater benefit from earning ISO 27001 certifications than large firms, and that more recent certifications are associated with greater positive abnormal returns than older certifications. Future research could provide a more detailed cross sectional analysis of this dataset in an effort to identify other situations/scenarios when significant investments in the development of a information security management program are met with abnormal stock market returns.

Two noted limitations of our study include the constrained sample size and the single country focus. First, although our sample size of 111 announcements provided sufficient power to detect statistical significance in our evaluations of every hypothesis, a larger sample size would further limit sampling error. Future researchers might consider incorporating additional security certifications or consider expanding the time horizon in an effort to develop a larger sample. Second, our results are based upon abnormal returns from two major American stock exchanges, so the same conclusions reached in our study may not apply to firms in countries with differing information security climates. Despite these limitations, we feel that our sample spans a significant breadth of industries and company sizes, making our results widely generalizable within the American economy and similar information security risk climates. However, we hope that future researchers will replicate this analysis for firms whose stock trades on foreign exchanges in an effort to expand our understanding of how this level of IS security investment is valued around the world.

While previous research has examined the impact of security breaches upon a firm [5–9], our study fulfills the need for empirical analysis on the value of the significant investment required to develop a robust information security program. Our findings indicate that the market perceives significant value in investments in this level of information security infrastructure. Though managers may hesitate to spend significantly on information security because of the difficulty in quantifying the preventative effects of those investments [40], our study provides empirical evidence for the market's valuation of investments in information security programs. In illuminating several insights on the market's response to ISO 27001 certification announcements, our research offers managers empirical guidelines with which to evaluate information security investment decisions within their firms.

References

1. Chen Y, Ramamurthy K, Wen K-W (2012) Organizations' information security policy compliance: stick or carrot approach? J Manag Inf Syst 29:157–188
2. Rainer RK Jr, Snyder CA, Carr HH (1991) Risk analysis for information technology. J Manag Inf Syst 8:129–147
3. Ligato L (2015) The 9 biggest data breaches of all time. Huffington Post
4. Volz D, Hosenball M (2016) Concerned by cyber threat. Obama seeks big increase in funding. Reuters, London
5. Campbell K, Gordon LA, Loeb MP, Zhou L (2003) The economic cost of publicly announced information security breaches: empirical evidence from the stock market. J Comput Secur 11:431–448
6. 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. Int J Electron Commer 9:70–104
7. Garg A, Curtis J, Halper H (2003) Quantifying the financial impact of IT security breaches. Inf Manag Comput Secur 11:74–83
8. Kannan K, Rees J, Sridhar S (2007) Market reactions to information security breach announcements: an empirical analysis. Int J Electron Commer 12:69–91
9. Malhotra A, Malhotra CK (2010) Evaluating customer information breaches as service failures: an event study approach. J Serv Res 14:44–59
10. Dos Santos BL, Peffers K, Mauer DC (1993) The impact of information technology investment announcements on the market value of the firm. Inf Syst Res 4:1–23
11. 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. Inf Syst Res 12:103–117
12. Von Solms R, Van Niekerk J (2013) From information security to cyber security. Comput Secur 38:97–102
13. Chai S, Kim M, Rao HR (2011) Firms' information security investment decisions: stock market evidence of investors' behavior. Decis Support Syst 50:651–661
14. Fama EF, Fisher L, Jensen MC, Roll R (1969) The adjustment of stock prices to new information. Int Econ Rev 10:1–21
15. Boehmer W (2008) Appraisal of the effectiveness and efficiency of an information security management system based on ISO 27001. In: The second international conference on emerging security information, systems and technologies. IEEE, pp 224–231
16. Brenner J (2007) ISO 27001: risk management and compliance. Risk Manag 54:24
17. Susanto H, Almunawar MN, Tuan YC (2011) Information security management system standards: a comparative study of the big five. Int J Electr Comput Sci 11:23–29
18. Hendricks KB, Singhal VR (1996) Quality awards and the market value of the firm: an empirical investigation. Manage Sci 42:415–436
19. Verizon (2015) 2015 data breach investigations report
20. Sen R, Borle S (2015) Estimating the contextual risk of data breach: an empirical approach. J Manag Inf Syst 32:314–341
21. Zhao X, Xue L, Whinston AB (2013) Managing interdependent information security risks: cyberinsurance, managed security services, and risk pooling arrangements. J Manag Inf Syst 30:123–152
22. Png IP, Wang C-Y, Wang Q-H (2008) The deterrent and displacement effects of information security enforcement: international evidence. J Manag Inf Syst 25:125–144
23. Kumar RL, Park S, Subramaniam C (2008) Understanding the value of countermeasure portfolios in information systems security. J Manag Inf Syst 25:241–280

24. Yue WT, Cakanyildirim M (2007) Intrusion prevention in information systems: reactive and proactive responses. J Manag Inf Syst 24:329–353
25. Udo GJ (2001) Privacy and security concerns as major barriers for e-commerce: a survey study. Inf Manag Comput Secur 9:165–174
26. Bulgurcu B, Cavusoglu H, Benbasat I (2010) Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS Q 34:523–548
27. Whitman ME (2003) Enemy at the gate: threats to information security. Commun ACM 46:91–95
28. Straub DW, Welke RJ (1998) Coping with systems risk: security planning models for management decision making. MIS Q 22:441–469
29. Gupta A, Zhdanov D (2012) Growth and sustainability of managed security services networks: an economic perspective. MIS Q 36:1109–1130
30. Wang C, Clark A (2013) HTC employees detained amid trade-secret investigation. Bloomberg, New York
31. Snider M (2013) Target data breach spurs lawsuits, investigations. USA Today, New York
32. Workman M, Bommer WH, Straub D (2008) Security lapses and the omission of information security measures: a threat control model and empirical test. Comput Hum Behav 24:2799–2816
33. Kwon J, Johnson ME (2014) Proactive versus reactive security investments in the healthcare sector. MIS Q 38:451–471
34. Gordon LA, Loeb MP (2002) The economics of information security investment. ACM Trans Inf Syst Secur 5:438–457
35. Agrawal M, Kishore R, Rao HR (2006) Market reactions to e-business outsourcing announcements: an event study. Inf Manag 43:861–873
36. Wang N, Liang H, Jia Y, Ge S, Xue Y, Wang Z (2016) Cloud computing research in the IS discipline: a citation/co-citation analysis. Decis Support Syst 86:35–47
37. Broadbent M (1998) Leveraging the new infrastructure: how market leaders capitalize on information technology. Harvard Business Press, Brighton
38. Whitman ME, Mattord HJ (2011) Principles of information security. Cengage Learning, Boston
39. Kelly L (2016) Making a return on IT security investment. Computer Weekly, London
40. Otim S, Dow KE, Grover V, Wong JA (2012) The impact of information technology investments on downside risk of the firm: alternative measurement of the business value of IT. J Manag Inf Syst 29:159–194
41. Wood CC (2004) Why information security is now multi-disciplinary, multi-departmental, and multi-organizational in nature. Comput Fraud Secur 2004:16–17
42. Verry J (2016) The rising cost of the ISO 27001 certification. PivotPoint Security, Trenton
43. Porter ME, Millar VE (1985) How information gives you competitive advantage. Harvard Bus Rev 63:149–160
44. Brown LD, Hagerman RL, Griffin PA, Zmijewski ME (1987) An evaluation of alternative proxies for the market's assessment of unexpected earnings. J Account Econ 9:159–193
45. Symantec (2014) Internet security threat report 2014
46. Fisher A, Kent C, Zage D, Jarocki J (2015) Using linkography to understand cyberattacks. In: 2015 IEEE conference on communications and network security (CNS). IEEE, pp 290–298
47. Ziobro P (2014) Target earnings slide 46% after data breach. Wall Str J
48. McWilliams A, Siegel D (1997) Event studies in management research: theoretical and empirical issues. Acad Manag J 40:626–657
49. Brown SJ, Warner JB (1985) Using daily stock returns: the case of event studies. J Financ Econ 14:3–31
50. Brown SJ, Warner JB (1980) Measuring security price performance. J Financ Econ 8:205–258
51. Konchitchki Y, O'Leary DE (2011) Event study methodologies in information systems research. Int J Account Inf Syst 12:99–115
52. Tanriverdi H, Uysal VB (2011) Cross-business information technology integration and acquirer value creation in corporate mergers and acquisitions. Inf Syst Res 22:703–720
53. Dewan S, Ren F (2007) Risk and return of information technology initiatives: evidence from electronic commerce announcements. Inf Syst Res 18:370–394
54. Mani D, Barua A, Whinston AB (2013) Outsourcing contracts and equity prices. Inf Syst Res 24:1028–1049
55. Bose I, Leung ACM (2014) Do phishing alerts impact global corporations? A firm value analysis. Decis Support Syst 64:67–78
56. Meng Z, Lee S-YT (2007) The value of IT to firms in a developing country in the catch-up process: an empirical comparison of China and the United States. Decis Support Syst 43:737–745
57. Bose I, Pal R (2012) Do green supply chain management initiatives impact stock prices of firms? Decis Support Syst 52:624–634
58. Bose I, Leung ACM (2013) The impact of adoption of identity theft countermeasures on firm value. Decis Support Syst 55:753–763
59. Armitage S (1995) Event study methods and evidence on their performance. J Econ Surv 9:25–52
60. Dodd P, Warner JB (1983) On corporate governance: a study of proxy contests. J Financ Econ 11:401–438
61. Binder J (1998) The event study methodology since 1969. Rev Quant Financ Acc 11:111–137
62. Kolari JW, Pynnonen S (2011) Nonparametric rank tests for event studies. J Empir Finance 18:953–971
63. Fama EF, French KR (1993) Common risk factors in the returns on stocks and bonds. J Financ Econ 33:3–56
64. Carhart MM (1997) On persistence in mutual fund performance. J Finance 52:57–82
65. MacKinlay AC (1997) Event studies in economics and finance. J Econ Lit 35:13–39
66. Willi FS, Knolmayer GF (2009) The effects of outsourcing announcements on market values of Swiss firms: an event study. Springer, Berlin
67. Berkman H, Truong C (2009) Event day 0? After-hours earnings announcements. J Account Res 47:71–103
68. Moeller SB, Schlingemann FP, Stulz RM (2004) Firm size and the gains from acquisitions. J Financ Econ 73:201–228
69. Ranganathan C, Brown CV (2006) ERP investments and the market value of firms: toward an understanding of influential ERP project variables. Inf Syst Res 17:145–161