The stock market impact of information security investments: The case of security standards

Dennis D. Malliouris and Andrew C. Simpson
Department of Computer Science, University of Oxford
Wolfson Building, Parks Road, Oxford OX1 3QD, UK

Abstract

Cyber security executives are inherently interested in developing, implementing, and reviewing cost-effective systems to safeguard their organisations from severe impacts of security breaches. Deciding which security projects to invest in can be a complex issue for such executives. One method that can help inform such decision making involves giving consideration to how the stock market reacts to security investments. One type of information security investment — complying with cyber security standards — is particularly interesting to consider, as these investments may not only have the potential to reduce financial penalties and losses associated with data breaches, but may also help to enhance reputation, win new business, and improve business processes. In this paper, we report upon a study that analysed the firm value impact of successful completion of such security investments by exploring two cases of cyber security certificates: the UK's Cyber Essentials scheme and the global ISO/IEC 27001 standard. 145 Cyber Essentials events between 2014 and 2018 and 76 ISO/IEC 27001 certifications between 2001 and 2018 were analysed. We find that the award of a Cyber Essentials (Plus) certificate is systematically associated with significant and positive market reactions. Surprisingly, our international sample reveals that becoming ISO/IEC 27001-compliant elicits significant negative abnormal stock returns. Potential explanations and implications of our findings are discussed.

1 Introduction

Security vulnerabilities and malicious actors pose a material threat to organisations in the 21st Century. In particular, for-profit organisations are rightfully concerned about data breaches. Due to a plethora of reasons, security breach impact, breach likelihood, and organisational resilience are difficult to quantify [1, 2]. Additionally, many surveys appear to follow agendas set by the organisations conducting these studies, resulting in exaggerated depictions of cybercrime realities [3]. Nevertheless, it is generally agreed that large-scale data breaches can prove costly to organisations.

Losses incurred by breached firms stem from lost revenues due to business disruptions, negative impacts on reputation, resources spent on investigation and recovery [4], as well as increased customer acquisition and retention costs, as customers who became victims of

fraudulent events are more likely to terminate the relationship and conduct business with competitors [5, 6]. There is a substantial body of literature on stock market reactions following security breaches. Using event study methodology, multiple studies demonstrated that security incidents are associated with statistically significant negative market reactions [7–18].

In order to manage and mitigate cyber security risks and prevent costly incidents from happening, firms may consider multiple alternatives geared towards enhancing their capabilities with regards to identifying, protecting their organisations from, detecting, responding to, and recovering from attacks [19]. For instance, organisations may opt to insure against risks, outsource cyber security, or invest in systems, processes, and staff [20]. Decision makers face difficulties in determining which investment projects should be pursued, how much should be invested into each one, and how the investment can be justified.

Maximising shareholder value is in the best personal and professional interest of a rational executive; it is also a major aspect of their fiduciary duty [21, 22]. Information security executives are thus incentivised to invest allocated budget in the most efficient way to enhance their firms' cash flows by reducing risk-adjusted losses or by generating returns greater than the investments [23]. Specifically, CSOs, CISOs, and similar executives aspire to invest in cost-effective measures to reduce the potentially costly impact of security breaches, improve operational and administrative processes, increase revenue due to enhanced trust, and convey a positive signalling effect to market participants.

What complicates matters is that the immediate return on information security investment is difficult to measure due to limited data availability and substantial dependence on qualitative judgements (see [24]). Therefore, only a small minority of firms evaluate their cyber security spending by means of calculating any post-investment metrics such as return on investment [25, 26].

One common type of cyber security investment executives may contemplate pursuing is security standards certification. Such certifications are an interesting type of investment to study for multiple reasons. First, they serve as a platform for (potentially substantial) secondary security investments. In order to become and remain compliant with security standards, prior investments in systems, people, and processes are required. Second, due to the fact that such standards cover multiple control areas, they have a greater potential to reduce security breach probabilities and costs than individual, disjoint discrete investments. Third, being awarded with a security standard certification implicitly carries a greater public-facing meaning. That is to say, a security certificate is an investment 'badge' that can be publicly displayed. Other, potentially more tangible (or more effective) security investments do not feature such an explicit signalling value, and hence do not offer the opportunity to enhance a firm's reputation. Moreover, given the inherent public-facing nature of security standards investments, they are particularly suitable to be studied using event study methodology.

In this paper, we consider two security standards: Cyber Essentials (Plus) and ISO/IEC 27001. These standards were chosen as they both provide firms with the potential advantages listed above. Specifically, both standards may: serve as guidelines for further investments; reduce security breach probabilities and costs; and convey a positive signalling value. However, despite their similarities, they differ significantly in terms of their governmental requirement, geographical reach, and comprehensiveness. Compliance with the Cyber Essentials programme is mandatory to become a supplier to many UK Government departments,

the programme is only intended for British companies, and it only demands that organisations meet a basic level of cyber security. An ISO/IEC 27001 certification is not required to bid for governmental contracts, the standard is globally applied, and it is more extensive in terms of its controls. Thus, the two standards create a favourable scenario for a study aspiring to establish generalisable results.

The aim is to investigate whether becoming certified according to Cyber Essentials (Plus) or ISO/IEC 27001 leads to material market reactions. We focus on successful awards of certification, as opposed to mere announcements of plans to become compliant. We consider certifications of entire organisations and subsidiaries to be events.

The remainder of this paper is structured as follows. First, in Section 2, we provide a summary of related literature and formulate our main hypothesis. Then, we describe the study's samples (Section 3) and the methodology applied (Section 4). Section 5 presents the empirical results obtained from our analysis, and Section 6 provides a discussion of the results. The paper concludes with a summary, final remarks, and a consideration of potential areas of further research.

2 Motivation

The aim of this paper is to investigate whether becoming certified according to Cyber Essentials (Plus) or ISO/IEC 27001 leads to significant market reactions.

2.1 Related Work

The work of Anderson and Moore [27,28] introduced economic considerations to information security research and practice. One aspect of relevance is information security investments. Information security executives' tasks include the planning, execution, and revision of security investments. To allocate resources economically, they require models, frameworks, and data to guide their decision-making process. Decision variables include, for example, the type, frequency, and intensity of cyber security investments [29,30].

Both conceptual and empirical research aiming to advance scholarly understanding of organisational behaviour in this regard has been conducted [24,29]. Taking into account the vulnerability of information confidentiality, integrity and availability, as well as the potential loss from such vulnerability, Gordon and Loeb [31] proposed an economic model to determine the optimal amount a firm should invest in information security. Contrary to intuition, they demonstrate that information security investments are only economical for medium levels of information vulnerability and only up to a limited fraction of the expected loss incurred by a security breach. Relatedly, Cavusoglu and colleagues [32] provide a comprehensive model for evaluating IT security investments. The authors also show that, with increasing quality of security systems, the cost of security decreases.

However, despite the value of such models, they do not effectively resolve the dilemma of reliably quantifying threat likelihood and impact. Moreover, while such models consider cyber risk mitigation, they tend to neglect potential secondary benefits obtained from investing in information security. Some empirical studies have attended to this latter issue

by evaluating value creation in terms of stock price reactions associated with organisational investment in information security.

Academic investigations of event-induced stock market reactions necessitate the validity of the efficient market hypothesis (EMH) in its semi-strong form [33, 34]. The semi-strong EMH postulates that stock prices reflect all publicly available information on the underlying firm and that they quickly adjust to the publication of additional news items. In the context of this paper, stock markets are considered to be semi-strongly efficient with respect to awards of security certificates (and entries in databases such as the ones used for this study) constituting or acting as news items.

Event studies analyse the extent to which actual stock market returns in firms differ from expected returns following a corporate event [35–39]. Here, the investment in information security is considered an event, and event study methodology is used to determine and assess abnormal returns. Event study methodology can be considered "the method of choice for analyzing market reactions to news" [40], and has frequently been used in the context of information economics (e.g. [40–42]).

The area of research investigating abnormal returns associated with information security investments builds on the strong body of literature on positive market reactions in terms of abnormal returns induced by general IT investments [43–48]. Based on this strand of literature, some researchers have analysed the short-term impact of IT security investments on the market value of the firm specifically. Generally, research on the corporate value implications of information security investments is scarce [16, 49]. These studies predominantly indicate a positive association between information security investments and stock prices. Applying event study methodology to a sample of 101 information security investment announcements of US firms between 1997 and 2006, Chai et al. [23] found significant positive abnormal returns of up to 1.89% [-2, 2]. Using generic search terms, such as 'information security' and 'information assurance', the authors covered a broad range of (unspecific) security investment types. Chai et al. [23] also demonstrated that information security investments with commercial exploitation and investments which took place after the introduction of the Sarbanes–Oxley Act are associated with higher abnormal returns. Their findings were corroborated in a later study which also demonstrated significant positive abnormal returns following security investments which can be commercially exploited, but significant negative abnormal returns upon investments which are exclusively intended for security improvements [50].

Bose and Leung [51] concentrated on a specific form of information security investment — identity theft countermeasures. Analysing events associated with "keywords such as anti-identity theft, 2FA, digital certificate, dynamic password generator, digital signature, and one-time password", they revealed statistically significant short-term mean cumulative abnormal stock returns of 0.63% following the announcement of such investments. The authors also showed that early adopters, and firms which invest in more sophisticated identity theft countermeasures, are associated with stronger positive short-term market returns.

Recently, Deane et al. [49] analysed the effect of 111 public announcements of successful ISO/IEC 27001 completions in the U.S. between 2005 and 2015. Analysing primarily new certifications (as opposed to re-certifications), the authors found that the announcement of successful ISO/IEC 27001 certifications in news media outlets such as Bloomberg and Reuters is associated with statistically significant positive abnormal returns. For instance,

in the event window including one day prior to the certification announcement and the event day/announcement day itself, the mean cumulative abnormal stock return was 0.72%.

However, there is also some contradictory evidence in the literature. Analysing 35 investments into cloud computing security following a cloud security breach from 2006 to 2010, one study finds a significant negative short-term impact on market value [52]. The authors also establish a negative spill-over effect following countermeasure investments, i.e. competitors' stock market value also decreases as a result of a focal firm's post-breach investment [52].

Jeong et al. [53] investigated 98 information security investment announcements between 2010 and 2017. They found no evidence of significant positive changes in market value following IT security investments. Additionally, the authors found their hypothesis that security investments create positive abnormal returns in competitors to be only partially supported [53]. Another study focusing on security investments of e-banking firms also provided weak evidence in support of the notion that security investments are not associated with statistically significant market value implications [54]. Finally, assessing 63 investment announcements under multiple timing scenarios, Szubartowicz and Schryen [55] reveal negative abnormal returns following the news of intended and accomplished investments into cyber security if these investments are not preceded by previous security incidents.

2.2 Hypothesis Development

Empirical research has demonstrated that voluntary and proactive security investments lead to fewer security failures [56]. Investments in cyber security standards can be considered a proactive type of investment given that they can constitute a platform for further systems, processes, and staff training in which firms may invest. A proactive approach towards acknowledging threats and taking steps to mitigate them also enables firms to generate higher revenues and focus more on core business activities [57]. Additionally, Liu et al. [58] showed that continuous investment in effective security countermeasures significantly reduces the probability of severe security incidents. Given the need to become re-certified annually (Cyber Essentials) or every three years (ISO/IEC 27001), certification facilitates continuous information security improvements and can thus be expected to reduce breach probabilities significantly. Given the potentially reduced breach probabilities and costs, investments in security can also lower cyber insurance premiums [59]. All aforementioned aspects might lead market participants to expect greater positive future cash flows.

However, despite the aforementioned positive aspects, there are potential caveats worth considering. First, Cyber Essentials controls do not cover all potential threats and attack vectors, which is why additional security investments might need to be made [60]. Moreover, in [60], it is empirically demonstrated that firms ought to exercise caution when implementing Cyber Essentials controls, as potential economic benefits might be eradicated quickly given the amount of time (and thus money) per machine invested. Relatedly, Bose and Leung [51] noted that effective security countermeasures are often associated with substantial costs, which may even prohibit firms from pursuing security investments.

In addition to high initial costs, firms are also likely to incur material follow-up costs. For instance, Moore et al. [25] noted that the ISO/IEC 27001 standard is frequently used by firms as a framework to guide future cyber security investments. Given the necessity to become re-certified after pre-defined periods of time and that security standards function

as a platform for further investments, market participants may rightfully expect substantial consequential costs stemming from further investments.

Prior research has demonstrated that firms which have suffered from a security breach are significantly more likely to invest in cyber security in the following year, and that security investments are positively associated with the probability of being attacked in the future [61]. Following an investment in certification, market participants might thus be inclined to assume that the investing firm did not publicise a previous breach. Moreover, although there is not necessarily a causal relation between security investments and attack frequency, malicious actors might become aware of the firm as a potential target, and investors might be reminded by a security investment that the focal firm is susceptible to security breaches.

From a shareholder's perspective, one might argue that a security breach is only relevant (and thus necessitating investments in countermeasures) if it leads to a significant negative share price impact. Despite the plethora of studies demonstrating that security incidents are associated with short-term negative abnormal returns (e.g. [16]), there is some evidence suggesting that such negative stock price shocks are only of short nature and do not impact firms in the long run [62,63]. Assuming that the share price impact of a security breach might be negligible, an investment in countermeasures might be perceived to be a waste of scarce economic resources. The considerations mentioned above might lead market participants to expect greater negative future cash flows.

In summary, investments in information security standards have the potential to reduce financial penalties and losses associated with data breaches, enhance reputation, win new business, and improve business processes. However, the initial investment is costly, necessitates follow-on expenses, and might conceivably be perceived as being associated with greater attack frequencies. In any case, we expect investors, analysts, and other market participants to alter their future cash flow expectations following investments in holistic security standards. Taking into account that existing research is inconclusive as to whether security investments are associated with significant (positive) abnormal returns, and that evidence suggests positive as well as negative future cash flows following initial investments in security standard certifications, ex ante, we do not assume directionality. Instead, in this study we aim to investigate whether becoming certified according to Cyber Essentials (Plus) or ISO/IEC 27001 leads to significant market reactions. To this end we hypothesise as follows:

> *The official certification of a firm with cyber security standards is associated with significant abnormal returns.*

3 Data Sources and Sample Characteristics

In order to analyse the predicted effect of security certificate investments on firms' stock prices, data regarding the selected types of standards needs to be collected. Generally, obtaining access to official databases on Cyber Essentials (Plus) and ISO/IEC 27001 certificates is difficult as certification bodies are generally (and understandably) reluctant to provide such data for competitive reasons.

Tables 1–3 presents descriptive statistics for the two samples used in the main analysis[1].

[1]Note: The ISO/IEC 27001 sample description is based on the event window [-3, 0]. Different sample

Table 1: Cyber Essentials (Plus) Sample

Year of certification	No. of certificates
2014	3
2015	14
2016	25
2017	56
2018	47
Total	145

Table 2: ISO/IEC 27001 Sample

Year of certification	No. of certificates
2011	1
2015	4
2016	15
2017	19
2018	37
Total	76

Table 4 shows descriptive statistics of the combined sample used in the subsequent regression analysis.

3.1 Cyber Essentials (Plus)

The UK Department for Business, Innovation and Skills launched the Cyber Essentials programme in 2014, intending to create a common minimum level of capabilities required by companies bidding for UK Government contracts involving the processing of sensitive and personal information. In its current form, the Cyber Essentials programme is operated by the National Cyber Security Centre (NCSC), which requires IT infrastructure compliance across five technical control categories: firewalls, secure configuration, user access control, malware protection, and patch management [64]. To achieve the Cyber Essentials Plus certification, compliance with the five technical controls is verified by one of five certification bodies appointed by the NCSC [65]. In order to retain certificate validity, the certification process needs to be undertaken annually [66].

First, a list containing all FTSE 350 Index constituents as of July 2018 was downloaded from *S&P Capital IQ*[2]. The analysis was restricted to organizations which have their primary listing on the London Stock Exchange as the Cyber Essentials programme is primarily aimed at British organisations. The 350 largest firms by market capitalisation were chosen as these index constituents are subject to coherent financial disclosure requirements, more closely followed by the public and financial analysts, and traded at greater liquidity — which facilitates more efficient incorporation of new pieces of information.

sizes across event windows are due to missing financial data points.

[2] `https://www.capitaliq.com/`

Table 3: ISO/IEC 27001 Sample

Country	No. of certificates	Country	No. of certificates
Australia	17	New Zealand	3
Austria	1	Nigeria	1
China	2	Oman	1
Denmark	1	Poland	1
France	1	Qatar	1
Germany	1	Singapore	1
Hong Kong	1	South Africa	2
India	9	Switzerland	2
Ireland	1	UAE	1
Japan	14	UK	2
Lebanon	1	US	9
Netherlands	1	Vietnam	2
Total			76

Second, a database containing (re-)certifications of FTSE 350 firms needed to be established. To this end, an unofficial database of firms granted a Cyber Essentials certificate had to be constructed. NCSC's Cyber Essentials website provides a list of accreditation bodies[3]. Two auditors issuing Cyber Essentials certificates, *CREST* and the associated firm *IT Governance*, provide lists of firms they certified[4][5]. These lists were downloaded as of July 2018. All FTSE 350 Index constituents were looked up in these lists of certified organisations provided by the two auditors to find associated certification events. Additionally, for every firm, a manual GCHQ certificate search[6] was conducted. Combining these two sources of data led to some conflicting data entries, particularly with regards to certificate issuance dates — in which cases priority was given to the GCHQ certificate search record. Neither database allowed us to differentiate between initial certifications and re-certifications. We consider both Cyber Essentials and Cyber Essentials Plus certificates in our analysis as the award of both requires cooperation with an official certification body.

For all certification events, the date of the respective certification, the certification type (Cyber Essentials or Cyber Essentials Plus), the name of the certified entity, its organisational hierarchical status (parent/holding company or subsidiary) and the source of the record (CREST/IT Governance, GCHQ, or both) were noted, which resulted in the final certification events database used. Event dates (i.e. days on which firms were certified according to the sources used) which fell on a non-trading day were adjusted to reflect the nearest trading day. We acknowledge that it is debatable whether this dataset represents a complete list of all certifications. Specifically, not all firms feature repetitive entries in our database, which suggests that not all firms seek re-certifications. However, the database constitutes a sufficiently large sample to test the hypothesised empirical relationship.

[3] `https://www.cyberessentials.ncsc.gov.uk/getting-certified/`

[4] `http://www.cyberessentials.org/list/`

[5] `https://www.itgovernance.co.uk/cyber-essentials-certified-organisations`

[6] `https://www.cyberessentials.ncsc.gov.uk/cert-search/`

This sample contains 145 certification events, of which 90 are Cyber Essentials and 55 are Cyber Essentials Plus (re-)certifications, respectively. Of these 145 events, 64 stem from the CREST/IT Governance list, 61 were found via the GCHQ certificate search, and 20 records were present in both types of sources. Within the sample, 66 events relate to parent/holding companies and the remaining ones to subsidiaries. The sample represents events in 62 firms across 38 different industries. The most frequent industries represented are Human Resource and Employment Services (29 events), Aerospace and Defence (20 events), and Asset Management and Custody Banks (11 events). Table 1 shows that there has been a constant year-over-year growth in certifications.

3.2 ISO/IEC 27001

ISO/IEC 27001, part of the ISO/IEC 27000 Information Security Management Systems family, provides internationally accepted requirements for Information Security Management Systems [67]. The standard features 114 controls across 14 clauses and objectives. The controls include, inter alia, requirements pertaining to access control, communications security, supplier relationship, incident management, and business continuity management. In order to demonstrate compliance with the standards, a company may announce it meets the requirements following an internal self-assessment. However, in order to fully benefit from potential advantages provided by the management system standard, companies may choose to become certified by an ISO-accredited certification body. To maintain an ISO/IEC 27001 certification, minor annual surveillance audits, as well as major recertification audits three years after the initial award, are required. The global number of organisations certified according to ISE/IEC 27001 standards in 2017 was 39,501 [68]. The ISO/IEC 27001 certificate has by now become a worldwide, widely accepted, standard for security certifications [69].

To create a sample of ISO/IEC 27001 certifications, a copy of the publicly available Certified Organisations Directory of the Joint Accreditation System of Australia and New Zealand (JAS-ANZ)[7] was downloaded in November 2018. The directory includes organisations certified by JAS-ANZ-accredited Certification Bodies[8] and thus features certified companies from multiple countries. All non-public companies were filtered out, which resulted in 84 certification events. For the remaining ones, additional corporate and financial information was downloaded from *S&P Capital IQ*. Excluding companies for which such information could not be found resulted in a usable sample of up to 76 events, out of which 18 ones relate to parent/holding companies, and 58 to certifications of subsidiaries, respectively. These events mainly constitute newly awarded certificates. Different sample sizes across event windows are due to missing financial data points. Table 3 shows that most (re-)certificates were awarded to companies headquartered in Australia (17) and Japan (14).

3.3 Combined Regression Sample

In order to further analyse potential firm and market characteristics influencing whether an investment in security standards is perceived favourably or unfavourably by market participants, a combined sample was constructed. Following the main analysis of Cyber Essentials

[7] `http://www.jas-anz.com.au/our-directory/certified-organisations`

[8] `http://www.jas-anz.com.au/about-the-jas-anz-register`

Table 4: Combined Regression Sample

Model		Model 1			Model 2			Model 3			Model 4	
Variable	Min	Mean	Max	Min	Mean	Max	Min	Mean	Max	Min	Mean	Max
Number of observations		219.00			219.00			217.00			198.00	
CAR [-2, 2]	-13.32	0.25	27.76	-13.32	0.25	27.76	-13.32	0.24	27.76	-13.32	0.27	27.76
Time (days)	0.00	1,110.20	1,613.00	0.00	1,110.20	1,613.00	0.00	1,108.00	1,611.00	20.00	1,114.00	1,611.00
Commercial and Professional Services (n)		50.00			50.00			50.00			50.00	
Consumer Services (n)		7.00			7.00			6.00			6.00	
Distributors (n)		6.00			6.00			6.00			6.00	
Financial services (n)		31.00			31.00			31.00			13.00	
Healthcare (n)		2.00			2.00			2.00			2.00	
Industrials (n)		46.00			46.00			46.00			46.00	
IT (n)		48.00			48.00			47.00			47.00	
Real Estate (n)		9.00			9.00			9.00			9.00	
Transportation (n)		12.00			12.00			12.00			12.00	
Utilities (n)		8.00			8.00			8.00			7.00	
CE (n)		145.00			145.00			144.00			130.00	
Log (total assets USDm)	1.97	8.58	14.70	1.97	8.58	14.70	1.97	8.58	14.70	1.97	8.42	13.90
Log (avg. daily volume)							-5.16	0.10	5.04	-5.16	0.04	4.14
Log (avg. PBV)							-1.11	1.15	3.22	-0.41	1.26	3.22
Positive EBITDA Growth (n)											97.00	
Australia (n)					16.00			16.00			15.00	
Austria (n)					1.00			1.00			1.00	
China (n)					2.00			2.00			2.00	
Denmark (n)					1.00			1.00			1.00	
France (n)					1.00			1.00			1.00	
Germany (n)					1.00			1.00			1.00	
Hong Kong (n)					1.00			1.00			1.00	
India (n)					9.00			9.00			9.00	
Ireland (n)					4.00			4.00			4.00	
Israel (n)					1.00			1.00			1.00	
Japan (n)					14.00			14.00			14.00	
Lebanon (n)					1.00			1.00				
Netherlands (n)					1.00			1.00			1.00	
Nigeria (n)					1.00			1.00				
New Zealand (n)					2.00			2.00			2.00	
Oman (n)					1.00			1.00				
Poland (n)					1.00			1.00			1.00	
Qatar (n)					1.00			1.00			1.00	
Singapore (n)					1.00			1.00			1.00	
South Africa (n)					2.00			2.00			1.00	
Switzerland (n)					2.00			2.00			2.00	
UAE (n)					1.00			1.00			1.00	
UK (n)					143.00			142.00			128.00	
USA (n)					9.00			8.00			8.00	
Vietname (n)					2.00			2.00			2.00	

(Plus) and ISO/IEC 27001 certifications, the two samples including the computed abnormal returns (see Section 4 below) were merged. Additionally, the following variables were downloaded from *S&P Capital IQ*: primary industry; total assets in USD million as per the most recent annual report prior to the certification event date; one-year-average daily volume of shares traded in millions of shares; one-year-average price-to-book ratio; and earnings before interests, tax, depreciation, and amortisation (EBITDA) as per the two most recent annual reports prior to the event date. Table 4 shows descriptive statistics for the variables used in the subsequent regression analysis. Note that the sample size decreases when including EBITDA growth due to data unavailability. Banks do not report EBITDA as their business model renders the figure meaningless.

4 Methodology

In this section we describe the methodology applied to our samples of cyber security standards certifications and illustrate one example for the analysis of abnormal returns following

Cyber Essentials certifications.

4.1 Analytical Procedure: Abnormal Returns Analysis

To establish abnormal stock price reactions following Cyber Essentials (Plus) and ISO/IEC 27001 certification events, standard event study methodology [35–39] was applied. Event studies can be considered the standard methodology to quantify immediate market reactions to news in the context of cyber security economics [40–42,51]. As rational market participants in efficient markets swiftly adjust their expectations of future cash flows, immediate market responses upon news reflect an assessment of current corporate activities' effect on future performance.

Share prices for all firms in the two samples were obtained from *S&P Capital IQ*. Daily returns were defined as

$$\frac{price_{i,t}}{price_{i,t-1}} - 1 \tag{1}$$

Here, $price_{i,t}$ is the share price of firm i on day t. For each certification event, n, expected returns were established using a one-factorial market model based on Sharpe's [70] single-index model[9], regressing individual firms' stock returns on the respective country's broad index[10] over the estimation window of 252 trading days. Using the market model, which assumes a linear relationship between stock return and market return, is common within the field of IT and information security investments [44, 51].

Event-specific coefficients were established via ordinary least square (OLS) regression. For each event, daily abnormal returns were defined as

$$\begin{aligned} AR_{i,t} &= R_{i,t} - E\left(R_{i,t}\right) \\ &= R_{i,t} - \left(\alpha_i + \beta_i R_{m,t} + \epsilon_i\right) \end{aligned} \tag{2}$$

Here, $AR_{i,t}$ denotes the abnormal return in security i on day t, $R_{i,t}$ the actual return in security i on day t, and $E(R_{i,t})$ the expected return for security i on day t. The coefficient α_i is the average stock return unrelated to market movements, β_i is the stock's sensitivity to returns of the index (defined as the covariance between the return of the stock and the return of the index divided by the variance of the index), $R_{m,t}$ is the daily return on the index, and ϵ_i is an unsystematic prediction error with an expected mean of zero.

Cumulative abnormal returns are defined as

$$CAR_i\left[t_I, t_{II}\right] = \sum_{t=t_I}^{t_{II}} AR_{i,t} \tag{3}$$

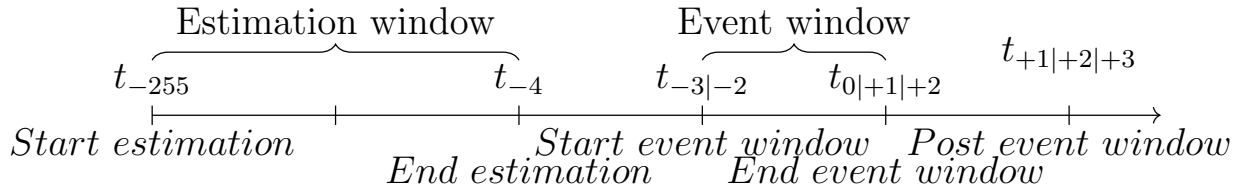
Here, $CAR_i\left[t_I, t_{II}\right]$ denotes the event-specific cumulative abnormal returns and t_I and t_{II} denote the beginning and end of the event window, respectively. To account for differences

[9] Sharpe's single-index model is theoretically grounded in fundamental financial theory laid out by Markowitz's Modern Portfolio Theory [71] and the work by Sharpe [72], Lintner [73], Treynor [74], and Mossin [75], respectively, which led to the formulation of the Capital Asset Pricing Model (CAPM).

[10] A list of all indices used can be obtained from the authors upon request.

in Cyber Essentials (Plus) certification dates across the sources, as well as for likely information leakage prior to the public announcement of a corporate event [49, 76, 77], we include market reactions of up to three trading days prior to the certification date in the analysis. Specifically, t_I — the start of an event window — is either the trading day three t_{-3} or two t_{-2} days prior to the certification date. Long event windows allow for a delay in market participants' correctly assessing and pricing in a new piece of information and may enable the respective event information to substantiate (e.g. the certified firm might fend off a large-scale cyber-attack more effectively than competitors, or it might win a government contract it would otherwise not have gained). However, as longer event windows increase the risk of including confounding events' share price impacts [76], we chose to analyse short event windows of up to two post-event days.

Hence, to measure short-term market reactions, event window end dates t_{II} were set to include the certification date, one, and two days following the certification date, respectively. The event windows are in line with those used in previous studies [23,49]. The timeline below illustrates estimation, event, and post-event windows' durations.



The reasoning for centring our study on the certification date, as opposed to the date of the announcement that a certification has been or will be pursued, is as follows. Although there might be stock market value implications stemming from the implementation of security standards prior to the official announcement [49], we conjecture that the official certification date constitutes the substantiation of actually being compliant with the respective standard. That is to say that only once an official certification body has independently and publicly announced that an organisation is certified according to a particular standard, potential customers can factor the certificate into their purchasing decisions. Consequently, only then may analysts, investors, and other market participants adjust their future cash-flow expectations and stock-price estimations accordingly. Similarly, market participants are likely to recognise breach probability and cost reduction potentials only after certifications have been officially granted by the respective bodies. Hence, it is reasonable to expect reductions in information asymmetries vis-à-vis information security capabilities (and thus positive share price reactions [78]) only after compliance with security standards has been conclusively established.

To mitigate the potential effect of outliers and to increase robustness, an additional measure of abnormal returns was introduced by winsorising cumulative abnormal returns in each of the two samples' event windows at the 0.15 level at each tail. To examine the statistical significance of unexpected share price behaviour following information security certifications, two-sided t-tests on all CARs' and winsorised CARs' means were performed to establish whether the population mean is significantly different from zero. Given the skewed distribution of individual event-specific CARs, non-parametric tests are likely to provide more reliable inferences in addition to parametric tests [39], and are commonly used in related literature (e.g. [9, 51]).

Accordingly, two additional non-parametric tests were conducted. First, sign tests on all event windows' CARs were performed to test whether the actual proportion of positive or negative cumulative abnormal returns to total number of observations exceeds the expected proportion. In line with MacKinlay [39] and the random walk hypothesis [34], the expected proportions were set at 0.5, which resembles an equal chance of obtaining positive or negative abnormal returns in a given period of time. The test statistics, *positive ratio* and *negative ratio*, were computed by dividing the number of events with positive or negative cumulative abnormal returns by the total number of observations in the respective subsample. Second, two-sided Wilcoxon signed-rank tests under the null hypothesis that the one-sample Hodges-Lehmann-type pseudo-median is equivalent to zero were performed on all samples [79, 80]. The parametric t-tests and non-parametric Wilcoxon signed-rank tests are non-directional to account for the fact that ex-ante it is not unambiguous whether the successful certification with a cyber security standard might be associated with any abnormal returns at all, not to mention the potential direction of such returns. Moreover, two-tailed testing can be considered more prudent and conservative (see, for example, [81]).

4.2 Illustration of Abnormal Returns Analysis

Consider the following example.

Capita plc had a Cyber Essentials re-certification in one of its subsidiaries, *Capita Business Services Ltd (CBSL)*, on 06/12/2017 (the event date). Expected returns were modelled by regressing *Capita plc*'s stock returns on the FTSE 350 during the period of time from 02/12/2016 to 30/11/2017. We estimate the event-specific β and α to be 0.49 and -0.0005, respectively. This implies that *Capita plc*'s stock is substantially less volatile than the market ($\beta < 1$) and that the firm's share price underperformed relative to the market ($\alpha < 0$).

As noted earlier, we assume that the efficient market hypothesis holds in its semi-strong form. Hence, analysts, investors and other market participants follow *Capita plc* and become aware of the Cyber Essentials re-certification. The following stock market reaction upon the completion of the security standard certification is due to market participants changing their future cash flow estimations. Consider, for instance, the event day itself. On 06/12/2017, the FTSE 350 returned 0.195%. According to Formula 2, the expected return on *Capita plc* is 0.039%. The actual stock return on the day was 0.787%, which leads to an abnormal return of 0.748%. By following this procedure over multiple trading days before and after the event day, and summing the respective daily abnormal returns, we compute a cumulative abnormal return of 4.129% for the event window $[-3, 2]$.

4.3 Analytical Procedure: Regression Analysis

To establish characteristics potentially affecting the perception of cyber security investments and hence abnormal returns as measured in our study, we examined eight variables in a subsequent regression analysis. In line with previous studies [23, 49, 51, 53] we considered the timing of an investment, the industry group in which a firm primarily operates, the type of certification, firm size, and growth potential. These characteristics can carry relevant implications about governance structures, IT maturity, and information asymmetries between the firm and its investors. Additionally, we also considered the country in which a firm is

located, its stock liquidity, and its EBITDA growth. The country in which a firm is headquartered defines the legal environment in which it operates. Stock liquidity is an indicator of how efficiently new pieces of information, such as certification news, can be incorporated into the stock price. Investors in a firm with negative EBITDA growth may be inclined to favour other types of investment of cyber security investments.

Timing of the investment is a relative measure and defined as the number of days passed since the first event date in the sample (24/06/2014). The 59 industries in which firms primarily operate were clustered into 11 industry groups[11]. Certification type was coded as a dummy variable (equal to 1, if the respective event is a Cyber Essentials (Plus) certification). Firm size is the natural logarithm of a firm's total assets in USD million as per the most recent annual report prior to the certification. Growth potential was computed as the natural logarithm of a firm's one-year-average price-to-book ratio (PBV, share price divided by book value per share), whereby a PBV greater than 1 implies that investors are valuing the respective firm higher than its net assets' worth. Liquidity was defined as the natural logarithm of the one-year-average[12] daily volume of shares traded in millions of shares. EBITDA growth is a dummy variable (equal to 1, if the EBITDA reported in the most recent annual report prior to the investment is greater than the EBITDA reported in the previous financial year).

In the first regression model, we examine the effect of timing, industry group, certification type, and firm size on abnormal returns following Cyber Essentials (Plus) and ISO/IEC 27001 certifications. In subsequent models, we add headquarters country, stock liquidity, growth potential, and EBITDA growth to the model. Coefficients were established via linear OLS regression. Across all models, the dependent variable are the post-certification event-specific cumulative abnormal returns in the event window $[-2, 2]$. The full model including all variables is defined as

$$\begin{aligned} CAR_{[-2,2]} = \beta_0 &+ \beta_1 Time + \beta_2 IndustryGroup + \beta_3 CertificationType + \beta_4 FirmSize \\ &+ \beta_5 StockLiquidity + \beta_6 GrowthPotential + \beta_7 EBITDAGrowth + \beta_8 Country \end{aligned} \tag{4}$$

5 Empirical Results

5.1 Overview

In this section we present the results of our analysis. Specifically, we analyse whether cumulative abnormal returns following security standards certifications are significantly different from zero by means of three statistical tests. Subsequently, we examine firm and market characteristics potentially affecting the direction and magnitude of abnormal returns.

We present all three statistical tests' results for both security standards and both outlier treatment approaches in the following order: Cyber Essentials (Plus) untransformed cumulative abnormal returns, Cyber Essentials (Plus) winsorised cumulative abnormal returns, ISO/IEC 27001 untransformed cumulative abnormal returns, and ISO/IEC 27001 winsorised

[11] A list detailing the industry clustering process can be obtained from the authors upon request.

[12] One year, starting on the respective event day, ending 365 days before the event date.

Table 5: Cyber Essentials (Plus) — Untransformed

Event window	n	M	Mdn	t	p_t	$PosRat$	p_{Sign}	$Pseudo\ Mdn$	$p_{Wilcoxon}$
$[-3, 0]$	145	0.751	0.091	2.138	0.034^{**}	0.545	0.159	0.257	0.152
$[-3, 2]$	145	1.056	0.201	2.545	0.012^{**}	0.545	0.159	0.351	0.110
$[-2, 1]$	145	0.591	0.087	1.938	0.055^{*}	0.531	0.253	0.141	0.439
$[-2, 2]$	145	0.749	0.346	2.084	0.039^{**}	0.545	0.159	0.262	0.224

Note: *** $p < 0.01$; ** $p < 0.05$; * $p < 0.1$; n = sample size; M = sample mean; Mdn = sample median; t = test statistics t-test; p_t = p-value t-test; $PosRat$ = positive ratio sign test; p_{Sign} = p-value sign test; $PseudoMdn$ = pseudo-median Wilcoxon test; $p_{Wilcoxon}$ = p-value Wilcoxon test. Mean and median cumulative abnormal returns are in percentage. t-tests and Wilcoxon signed-rank tests are two-sided, testing the alternative hypothesis that the population mean is different from zero and that the population pseudo-median is different from zero, respectively. Sign tests are one-sided, testing the alternative hypothesis that the positive ratio is greater than chance (0.5).

cumulative abnormal returns. In each table, two-sided t-test, one-sided sign test, and two-sided Wilcoxon signed-rank test results are shown for four event windows, which cover the event day, as well as up to three trading days prior to and up to two trading days following a certification date. Within each table, from left to right, the columns indicate the event window under consideration, the number of certification events in the respective event window, the sample mean and median, and test statistics and associated p-values for t-tests, sign tests and Wilcoxon signed-rank tests. Statistical significance is accepted at p-values below 0.05; statistical trends at p-values of less than 0.1 are also discussed.

In Section 5.4 we present results obtained from the regression analysis. Abnormal returns in the event window $CAR[-2, 2]$ are defined as the outcome variable across all models. Each regression model includes different sets of regressors. Model (1) examines timing, industry group, certification type, and firm size. Model (2) also includes the country in which a firm is headquartered. Model (3) additionally considers stock liquidity and growth potential. In the full model (4), we also add EBITDA growth. For each model and regressor, the estimated coefficients are shown, with standard errors in parentheses.

Overall, we find that the award of Cyber Essentials (Plus) certificates is associated with economically and statistically significant *positive* abnormal returns. In contrast, ISO/IEC 27001 certificate awards are coherently associated with economically and statistically significant *negative* abnormal returns. The regression analysis demonstrates limited positive relations between abnormal returns and time, Cyber Essentials certificates, firm size, and firms headquartered in Nigeria, respectively. The models also reveal limited negative associations between abnormal returns and Financial Services, Industrials, and IT firms, respectively.

5.2 Cyber Essentials (Plus)

Table 5 presents the analysis of untransformed abnormal returns following Cyber Essentials (Plus) certifications. The t-test results almost unanimously show that CAR scores are statistically significantly different from zero with positive mean CARs across all four event windows. For instance, the mean $CAR[-3, 2]$ is 1.06% ($n = 145, p = 0.012$), which is also

Table 6: Cyber Essentials (Plus) — Winsorised

Event window	n	M	Mdn	t	p_t	$PosRat$	p_{Sign}	$Pseudo\ Mdn$	$p_{Wilcoxon}$
$[-3, 0]$	145	0.298	0.091	2.334	0.021^{**}	0.545	0.159	0.337	0.023^{**}
$[-3, 2]$	145	0.304	0.201	2.023	0.045^{**}	0.545	0.159	0.312	0.046^{**}
$[-2, 1]$	145	0.063	0.087	0.499	0.619	0.531	0.253	-0.007	0.976
$[-2, 2]$	145	0.198	0.346	1.285	0.201	0.545	0.159	0.146	0.128

economically significant. Only the mean CAR of the four-day event window $[-2, 1]$ suggests merely a statistical trend of CARs being statistically significantly different from zero. It can also be observed that mean CARs become more positive over time, i.e. the longer event windows $[-3, 2]$ and $[-2, 2]$ are associated with greater abnormal returns than the event windows $[-3, 0]$ and $[-2, 1]$ are.

The non-parametric tests do not support initial indications as provided by the parametric t-test. In absolute terms, all sign tests' positive ratios are greater than 50%, which means that more than half of all Cyber Essentials (Plus) certification events are coherently associated with positive cumulative abnormal returns. However, no sign test provides sufficient evidence to reject the null hypothesis that the actual proportion of positive CARs statistically significantly exceeds chance. Interestingly, there is almost no change in positive ratios and associated p-values across the event windows, indicating that abnormal returns in a given firm are coherently positive or negative over time.

Similarly, the non-parametric Wilcoxon signed-rank test does not provide further evidence for the presence of positive abnormal returns following Cyber Essentials (Plus) certifications. For untransformed CARs, the two-sided test results indicate that CARs are not statistically significantly different from zero during the four considered event windows, although all (pseudo-)medians are substantially positive.

The analysis of winsorised abnormal returns following Cyber Essentials (Plus) certifications is shown in Table 6. Mean and median winsorised CARs are positive across all event windows. For a given event window time frame, winsorised mean CARs tend to be lower than untransformed mean CARs, which can suggest the presence of outliers featuring strong positive market reactions subsequent to security certification events. Notwithstanding the lower magnitude of winsorised mean CARs scores, their t-tests corroborate initial observations for untransformed scores. After reducing the impact of outliers, the four- and six-day event windows starting at $[-3]$ continue to exhibit statistically significant positive mean CARs. For instance, the winsorised mean $CAR[-3, 2]$ is 0.30% ($n = 145, p = 0.045$). The aforementioned observation that abnormal returns increase over time also holds in the case of winsorised scores.

As winsorising does not alter the number of positive event-specific CARs, the positive ratio and sign test results remain unchanged relative to the untransformed figures.

The non-parametric Wilcoxon signed-rank test for winsorised CARs provides evidence in support of the hypothesis that certification events are followed by significant abnormal returns. Following the outlier treatment, CARs in the event windows $[-3, 0]$ and $[-3, 2]$ appear to be statistically significantly different from zero and positive. For instance, the

Table 7: ISO/IEC 27001 — Untransformed

Event window	n	M	Mdn	t	p_t	$NegRat$	p_{Sign}	$Pseudo\ Mdn$	$p_{Wilcoxon}$
$[-3, 0]$	76	-0.875	-0.374	-2.077	0.041^{**}	0.671	0.002^{***}	-0.643	0.056^{*}
$[-3, 2]$	74	-1.165	-0.921	-2.324	0.023^{**}	0.703	$<0.001^{***}$	-0.901	0.020^{**}
$[-2, 1]$	75	-0.449	-0.440	-1.562	0.123	0.667	0.003^{***}	-0.377	0.186
$[-2, 2]$	75	-0.795	-0.704	-2.064	0.043^{**}	0.693	0.001^{***}	-0.640	0.054^{*}

Note: *** $p < 0.01$; ** $p < 0.05$; * $p < 0.1$; n = sample size; M = sample mean; Mdn = sample median; t = test statistics t-test; p_t = p-value t-test; $NegRat$ = negative ratio sign test; p_{Sign} = p-value sign test; $PseudoMdn$ = pseudo-median Wilcoxon test; $p_{Wilcoxon}$ = p-value Wilcoxon test.
Mean and median cumulative abnormal returns are in percentage. t-tests and Wilcoxon signed-rank tests are two-sided, testing the alternative hypothesis that the population mean is different from zero and that the population pseudo-median is different from zero, respectively. Sign tests are one-sided, testing the alternative hypothesis that the negative ratio is greater than chance (0.5).

winsorised median $CAR[-3, 2]$ is 0.20% ($n = 145, p = 0.046$).

5.3 ISO/IEC 27001

Test results concerning abnormal returns following ISO 27001 certifications presented in Tables 7 and 8 provide a more unified picture as both parametric and non-parametric CARs are significantly negative. Table 7 displays test results for untransformed abnormal returns.

All mean CARs are negative across all four event windows. T-test results indicate that mean CARs in all but one event window are statistically significantly different from zero. For instance, the mean $CAR[-3, 2]$ is -1.17% ($n = 74, p = 0.02$), which is also economically material. Mean CARs following ISO 27001 certifications become more negative with increasing event window lengths, i.e. mean CARs in event windows $[-3, 2]$ and $[-2, 2]$ are more negative than the CARs in event windows $[-3, 0]$ and $[-2, 1]$, respectively.

Sign test results confirm the t-test results. Negative ratios range from $0.67[-2, 1]$ to $0.70[-3, 2]$, with p-values indicating that in every considered event window, negative CARs are statistically significantly more likely to occur than by mere chance.

Median CARs are also negative for all event windows and range between -0.37% $[-3, 0]$ and -0.92% $[-3, 2]$. Wilcoxon signed-rank test results for untransformed CAR scores indicate that the true median CAR in the event windows $[-3, 2]$ is indeed different from zero ($n = 74, p = 0.02$). For the event windows $[-3, 0]$ and $[-2, 2]$, we find strong statistical trends suggesting that the true median CAR is materially negative in these event windows as well.

Statistical test results for winsorised abnormal returns following ISO 27001 certifications are shown in Table 8 and strongly support inferences drawn from the prior analysis of untransformed abnormal returns.

All winsorised mean CARs are negative across event windows. In each event window, winsorised mean CARs are slightly less negative than untransformed CARs. T-tests on winsorised CARs uniformly support the notion that the population mean is negative and statistically significantly different from zero. For instance, the winsorised mean $CAR[-3, 2]$ is -1.17% ($n = 74, p = 0.001$), which is also strongly economically significant. Again, negative

Table 8: ISO/IEC 27001 — Winsorised

Event window	n	M	Mdn	t	p_t	$NegRat$	p_{Sign}	$Pseudo\ Mdn$	$p_{Wilcoxon}$
$[-3, 0]$	76	-0.687	-0.374	-3.069	0.003^{***}	0.671	0.002^{***}	-0.748	0.012^{**}
$[-3, 2]$	74	-0.935	-0.921	-3.475	0.001^{***}	0.703	$<0.001^{***}$	-1.043	0.002^{***}
$[-2, 1]$	75	-0.438	-0.440	-2.385	0.020^{**}	0.667	0.003^{***}	-0.517	0.066^{*}
$[-2, 2]$	75	-0.653	-0.704	-2.857	0.006^{***}	0.693	0.001^{***}	-0.678	0.011^{**}

abnormal returns become more substantial over time.

Mitigating outliers through winsorising does not alter the number of negative event-specific CARs, hence the negative ratio and sign test results remain unchanged relative to the untransformed figures.

Winsorised median CAR scores also remain unchanged relative to the untransformed figures and are hence negative across all event windows. After mitigating the effect of outliers, the Wilcoxon sign-ranked test results indicate that winsorised CAR scores reveal an even greater tendency to be statistically significantly different from zero than their untransformed counterparts. Specifically, the true median CARs in the event windows $[-3, 0]$, $[-3, 2]$, and $[-2, 2]$ appear to be statistically significantly different from zero. For the event window $[-2, 1]$ we find a strong statistical trend suggesting that the true median CAR is materially negative in this event window as well.

5.4 Regression Analysis

Table 9 presents the regression analysis results. Only model (1) is overall-significant as per the F-Test of Overall Significance. The model reveals a statistically significant and negative association between abnormal returns in the event window $CAR[-2, 2]$ and the Financial Services, Industrials, and IT industries. There is also limited statistical evidence suggesting a positive relation between the abnormal returns and time, Cyber Essentials certificates, and firm size. In models (2) to (4), the empirical effect of the three aforementioned industries persists, although less pronounced. In these models, the negative effect of firms primarily operating in the IT industry merely becomes a statistical trend. The same holds for model (4) and the Financial Services industry's effect. Surprisingly, none of the countries apart from Nigeria (in models (2) and (3)) display a statistically significant effect on abnormal returns. According to these models, firms headquartered in Nigeria are associated with more positive abnormal returns following investments in security standards.

5.5 Summary

Overall, the evidence regarding Cyber Essentials (Plus) certifications is mixed. T-tests of untransformed CARs suggest the presence of positive abnormal returns significantly different from zero across all event windows. However, these results are not supported by non-parametric tests. When mitigating the influence of outliers, significant and positive abnormal returns appear to be present in the event windows $[-3, 0]$ and $[-3, 2]$ as per t-tests

Table 9: Regression Results

	Dependent variable:			
	CAR[-2,2]			
	(1)	(2)	(3)	(4)
Time	0.001*	0.001	0.001	0.001
	(0.001)	(0.001)	(0.001)	(0.001)
Industry dummies included Selected coefficients shown	Yes	Yes	Yes	Yes
Financial services	−2.359**	−2.718***	−2.894**	−2.845*
	(0.937)	(1.036)	(1.195)	(1.492)
Industrials	−2.414***	−2.656***	−2.727***	−2.791***
	(0.812)	(0.851)	(0.923)	(0.972)
IT	−1.978**	−1.958*	−2.025*	−1.963*
	(0.882)	(0.994)	(1.049)	(1.093)
Certification Type	1.149*	4.377	4.314	4.353
	(0.650)	(3.241)	(3.302)	(3.434)
Firm Size	0.267*	0.189	0.408	0.432
	(0.145)	(0.166)	(0.295)	(0.329)
Stock Liquidity			−0.272	−0.307
			(0.318)	(0.352)
Growth Potential			0.161	0.102
			(0.454)	(0.514)
EBITDA Growth				−0.090
				(0.663)
Country dummies included Selected coefficient shown	No	Yes	Yes	Yes
Nigeria		8.693**	9.476**	
		(4.264)	(4.425)	
Constant	−2.864	−2.616	−4.256	−4.155
	(1.803)	(2.088)	(2.918)	(3.193)
Observations	219	219	217	198
R^2	0.103	0.166	0.170	0.160
Adjusted R^2	0.051	0.001	-0.007	-0.027
Residual Std. Error	3.964 (df = 206)	4.068 (df = 182)	4.101 (df = 178)	4.226 (df = 161)
F Statistic	1.978** (df = 12; 206)	1.006 (df = 36; 182)	0.962 (df = 38; 178)	0.854 (df = 36; 161)
Note:				*p<0.1; **p<0.05; ***p<0.01

and Wilcoxon signed-rank tests. This leads us to consider, in this case, that the main hypothesis — the completion of security standards is associated with significant abnormal returns — to be only partially supported. We deduce that Cyber Essentials (Plus) certifications can be associated with significant positive abnormal returns.

In contrast, we find strong evidence suggesting a negative association between ISO/IEC 27001 certifications and short-term stock market returns. Negative untransformed and winsorised mean CARs can be observed across all event windows. Together with t-tests suggesting statistically significant deviance from zero, this demonstrates that, on average, ISO/IEC 27001 awards are followed by negative market reactions. Both non-parametric tests corroborate these t-test results substantially. Consequently, we consider, in this case, that our main hypothesis — the completion of security standards is associated with significant abnormal returns — to be fully supported.

In summary, we find that completed investments in information assurance standards elicits statistically significant stock market reactions. Surprisingly, the results for the two types of certificates point in diametrically opposed directions: the completion of Cyber Essentials (Plus) certifications can increase a firm's share price, whereas becoming compliant with the ISO/IEC 27001 standard is likely to diminish a firm's market value. The subsequent regression analysis only contributes a limited amount of additional insights to the counterintuitive results. We find that Financial Services, Industrials, and IT firms are negatively associated with abnormal returns, whilst Cyber Essentials certificates, time, and firm size have a positive impact on $CARs[-2, 2]$.

6 Discussion

Our literature review revealed an absence of a consensus as to whether security investments create value as indicated by significant positive abnormal returns. Moreover, we find antithetic evidence suggesting that security investments might indeed be associated with negative future cash flows and thus negative abnormal returns. In any case, we expect investors, analysts, and other market participants to alter their future cash flow expectations following investments in holistic security standards. If these economic agents expect future economic benefits stemming from the investment to be greater than the associated costs, share prices will increase following successful security certifications. On the other hand, if stock market participants anticipate initial and follow-on costs associated with the investment to be greater than future benefits, share prices will decrease following successful security certifications. Accordingly, we hypothesised that the certification of a firm with a cyber security standard is associated with significant abnormal returns. To investigate our hypothesis we gathered data on two different types of information security standards and conducted an event study to examine the immediate impact of a security investment on stock prices and thereby the respective firm's market value. We consider the results of Section 5 below.

6.1 Cyber Essentials (Plus)

The data analysis showed that investing into Cyber Essentials (Plus) certifications resulted in abnormal returns of up to 1.06% over the six-day period starting three trading days prior

to the certification date and ending two trading days afterwards. Positive abnormal returns following these certifications are statistically significant according to parametric tests. Winsorised abnormal returns corroborate the finding and also indicate statistical significance according to the non-parametric Wilcoxon signed-rank test. Market reactions following Cyber Essentials investments are thus in line with previous studies [23, 51]. The significant positive abnormal returns following Cyber Essentials certifications indicate that investors expect economic benefits of the investment to outweigh associated costs (i.e. more positive cash flows). Potential reasons for stock market participants' positive re-valuation of firms may include their believe that becoming Cyber Essentials-compliant can reduced financial penalties and losses associated with data breaches, enhance reputation, elicit greater revenues, and facilitate business process improvements.

It is worth reiterating that compliance with the Cyber Essentials programme is necessary to bid for "government contracts which involve handling of sensitive and personal information and provision of certain technical products and services" [82]. It is plausible to assume that investors pay particular attention to the fact that only certified firms are allowed to bid for particular UK Government contracts, and that there is thus a direct positive cash flow component to becoming Cyber Essentials-compliant. This conjecture is echoed by the finding that security investments with commercial exploitability are associated with greater abnormal returns than those exclusively intended for security improvements [23, 50]. In fact, the types of industries predominantly present in our sample (Human Resources and Employment Services and Aerospace and Defence) suggest that firms aspiring to comply with the Cyber Essentials programme mainly do so to become and/or remain UK Government suppliers. Our sample might hence be biased due to this self-selection process.

Firms operating within the Human Resources and Employment Services industry by definition handle personal information, whilst those active in the Aerospace and Defence industry naturally provide technical products and services of high relevance to government customers. Whilst it is difficult to link changes in financial performance directly to security standards certifications — as such strategic decisions do not take place in isolation and cannot be analysed ceteris paribus — it is unambiguous that absence of Cyber Essentials certifications prohibits firms from bidding for certain government contracts, and some firms might find it difficult to operate profitably without winning these contracts.

Consider, for example, British company *G4S plc*. The company, inter alia, provides prison and airport security services, and engages in other high-level security tasks for the UK Government. As a public services outsourcing company, it is highly dependent on government contracts[13]. Being compliant with a security standard required to bid for government contracts is a necessity for such firms, which are thus highly incentivised to pursue the respective certification. Once a firm such as G4S becomes (re-)certified according to Cyber Essentials standards, it can expect greater future revenues relative to hypothetical future revenues without being compliant to the information security standard. Market participants are likely to expect that additional revenues generated by firms known to be government suppliers/contractors exceed associated security certificate investment expenses. Such investors would in turn highly appreciate firms pursuing Cyber Essentials certifications, and hence acknowledge security standards certifications with greater share prices, resulting in

[13] `https://www.ft.com/content/daea0a2e-4496-11e9-b168-96a37d002cd3`

positive abnormal returns. Anecdotally, this can indeed be observed for *G4S plc*. The firm's Cyber Essentials certification events, elicit an average $CAR[-2, 1]$ of 2.08%.

Additionally, our Cyber Essentials (Plus) sample does not differentiate between new certifications, initial subsidiary certifications, follow-on certifications of the entire organisation, and mandatory later re-certifications. Positive mean abnormal returns found in our sample might thus stem from the fact that market participants deem follow-on company-level certifications and re-certifications economically reasonable as they allow for a (continuous) ability to bid for UK Government contracts without necessitating substantial new investments in IT controls.

Overall, in light of the security and firm value benefits, from a security executive's perspective, it makes economic sense to invest in becoming Cyber Essentials (Plus) certified.

6.2 ISO/IEC 27001

On the contrary, our ISO/IEC 27001 analysis reveals that the certification is coherently associated with significant negative abnormal returns of up to -1.16% over the six-day period starting three trading days prior to the certification date and ending two trading days afterwards. Negative mean abnormal returns persist across all event windows and are statistically significant according to both parametric and non-parametric tests in both outlier treatment approaches. These statistically significant negative returns following ISO/IEC 27001 certifications suggest that market participants expect the security standard to entail substantial initial and follow-on costs which are not exceeded by savings stemming from reduced security breach probabilities and costs. Anticipating follow-on costs to be greater than those associated with the Cyber Essentials programme is reasonable. Whilst both security standards function as platforms for further investments, the ISO/IEC 27001 standard features 114 controls, which may necessitate greater costs to maintain and advance.

We identify multiple additional potential reasons for the negative stock market reaction. First, Jeong et al. [53] argued that the absence of positive market reactions following security investments can be due to market participants already expecting firms to invest in security. Investors do not consider news of substantial investments a differentiator, but, rather, a cost factor. Accordingly, an investment in ISO/IEC 27001 controls might merely be deemed a compulsory exercise, and it might constitute a negative surprise to investors that a particular firm has not already made necessary investments before.

Another likely explanation is that market participants do not appreciate the necessity to invest in cyber security. Szubartowicz and Schryen [55] contend that prior to a security breach, market participants might consider security investments not worth pursuing and therefore react negatively upon intended and completed security investments. Therefore, investors might consider an ISO/IEC 27001 certification — a major long-term investment endeavour — unnecessary for companies which have not yet experienced a severe security incidents.

Another important difference to note vis-à-vis our analysis of the Cyber Essentials programme is that the sampling process of ISO/IEC 27001 events centred on newly issued certificates, whereas the Cyber Essentials (Plus) sample contains multiple re-certificates. Negative market reactions should therefore be viewed as associated with the substantial initial investment. Accordingly, investors might perceive later re-certifications more positively,

as these convey a positive signalling effect regarding the firm's cyber security capabilities without necessitating substantial new investments in IT controls.

As our results contradict those established by an earlier study on market value implications of ISO/IEC 27001 completions [49], we conjecture that there may be significant regional differences. Deane et al. [49] demonstrated statistically significant positive abnormal returns on the U.S. stock market following ISO/IEC 27001 certifications. The divergence might be caused by different levels of market sophistication and liquidity. The U.S. stock market can be considered fairly developed and efficient, whereas, for instance, emerging and developing markets might behave differently. This notion is in line with the finding that, in the U.S., stock market, participants reacted with even more positive abnormal returns to security investments after the introduction of the Sarbanes–Oxley Act, a major accounting and transparency reform, than before [23]. Moreover, differences between the results obtained for the Cyber Essentials programme relative to the ISO/IEC 27001 standard can be due to asset liquidity. FTSE 350 stocks can be considered highly liquid, whereas markets in developing countries may be too illiquid to react to security investments in a similar manner.

Notwithstanding potential explanations, these results are interesting and potentially discouraging for a security executive contemplating an investment in ISO/IEC 27001 controls. However, the results neither implicate that (investors believe that) the security controls are ineffective, nor do they convey information about long-term firm value implications. Regardless of the negative short-term abnormal returns, pursuing investments in ISO/IEC 27001 certificates is thus not necessarily economically unreasonable.

6.3 Regression Analysis

The subsequent regression analysis only yields limited additional insights into the counterintuitive results. Only one regression model can be considered overall-significant. Regression models (2) to (4) are not statistically significant overall due to the introduction of country-dummy variables. Country-level (and to a limited extend also industry-level) subsamples are too small to yield substantial insights.

Across all models, we find a persistent negative association between Financial Services, Industrials, and IT industries and abnormal returns following security standard certifications. In the overall-significant model, time and firm size appear to have a small positive impact on abnormal returns. Additionally, in models (2) and (3), out of all countries, only Nigeria is significantly and positively associated with post-certification abnormal returns.

The persistent negative association between the three industries and post-certification abnormal returns merits particular discussion. From the regression results it appears as though investors in Financial Services, Industrials, and IT firms do not expect reduced breach costs to outweigh initial and follow-on investment expenses. In the case of Financial Services and Industrials firms, investors might deem security standards investments to be ineffective and to require substantial follow-on expenses given the complexity of the firms' operations, their large attack surface, and the value of their data. In the case of the IT industry, market participants might consider firms inherently experienced in information security matters and do thus not appreciate (seemingly redundant) investments in the protection of information confidentiality, integrity, and availability.

The positive impact of time on abnormal returns elicited by investments in security certificates suggests that over the course of time, market participants react more favourably to firms pursuing security standards investments. This might be due to investors, for instance, by increasing media coverage, becoming more knowledgeable about security threats, associated costs, and the necessity to mitigate them.

The positive coefficient for the variable certification type corroborates earlier findings discussed above. Cyber Security (Plus) certifications tend to be associated with more positive abnormal returns than ISO/IEC 27001 certifications.

Firm size's positive impact on abnormal returns somewhat contradicts previous findings [49], and may be due to market participants expecting economic benefits from security standards to exceed associated costs at larger firms. The positive impact of size might also stem from reduced ex-ante information asymmetries. Larger firms tend to be followed more extensively by analysts and the media, and it is thus likely that larger firms' security certification news are disseminated more efficiently.

Nigeria's positive association with abnormal returns can potentially be interpreted as an indicator that, in less-mature markets, external certifications carry an even higher relevance than they do in highly-developed markets.

6.4 Limitations

There are some limitations to our study.

First, the major constraints stem from the methodology used (see [40]). Event studies can only reliably generate evidence of short-term stock market reactions. Given that security investments may only prove appropriate in the long-run, the immediate nature of market reactions might not prove a helpful metric to inform decision-making processes. Moreover, given the constant stream of new information to be factored in by stock market participants, there is an abundance of confounding events that may affect organisations' market value but are impossible to control for.

Additionally, abnormal returns upon the listing of compliance may only represent a proportion of the overall stock market reaction associated with investments in security standards. It is indeed likely that the notification of the decision to pursue an investment, the announcement of having completed an investment, and the actual official listing in a database all generate discrete changes in a firm's market value. Accordingly, a negative market reaction on the certification day may merely offset an initial positive overreaction on the day of the announcement that a security certificate investment will be pursued. Relatedly, abnormal returns across studies are difficult to compare given that other studies (e.g. [49, 51]) centre their event studies on announcement dates, whereas we utilise actual certification dates.

Finally, abnormal returns following Cyber Essentials (Plus) and ISO/IEC 27001 certifications are difficult to compare on a like-for-like basis as, for example, our sample of Cyber Essentials events contains re-certifications, whereas the ISO/IEC 27001 analysis focuses on newly issued certificates.

7 Conclusions and Future Research

The presence of significant abnormal returns might provide corporate decision makers with an indication as to how market participants perceive this type of security investment. Consequently, the results of our investigation may inform organisational security budget allocation. Analysing 145 Cyber Essentials and 76 ISO/IEC 27001 certification events, we find that Cyber Essentials (Plus) certifications are associated with significant positive abnormal returns, whereas ISO/IEC 27001 certifications are associated with significant negative abnormal returns. The results imply that market participants expect positive cash flows to follow from Cyber Essentials certifications and diminished cash flows as a consequence of ISO/IEC 27001 investments.

UK-based policy makers might find our study helpful to reduce negative externalities caused to society by companies not securing their data. Firms which can externalise breach costs to society are not incentivised to invest in attack deterrence and hence invest more in damage control than in breach avoidance [20]. Policy makers such as the NCSC might want to encourage more companies to actively manage cyber risk by investing in Cyber Security (Plus) controls. Demonstrating positive firm value implications in addition to reduced breach probability and costs might support such endeavours.

For security executives contemplating investments in ISO/IEC 27001 certificates, the purpose of this study is not to discourage them from doing so, despite demonstrating the existence of negative stock market reactions following completed certifications in our sample. The Information Security Management Systems standard is comprehensive and guided by security experts and academics. Such holistic improvements of information security are supposed to reduce future breach probability and costs [49, 69]. Our findings are rather intended to encourage companies to improve their security communication processes, for instance, by informing market participants about the advantages of the certification for their firms. Moreover, firms should pay particular attention to actively managing initial and follow-on costs associated with the certification.

In future studies, we intend to enlarge our sample and include more events, firms, and countries to verify the robustness and generalisability of our findings. With regards to the ambivalent nature of our results, future research should replicate the present study on other financial markets and take into account other certificates. Furthermore, in an extended version of the present study, one could also consider re-classifying the timing of certification events' occurrence (e.g. considering publications of news items on certifications to be the event date as opposed to auditors' award dates).

Additionally, given that our study is primarily of an exploratory nature, in future work, we aim to expand our initial cross-sectional analysis to dissect factors which contribute to positive and negative abnormal returns, respectively. First, we aim to extend the thesis that greater abnormal returns induced by Cyber Essentials certificates are due to the certificate's commercial exploitability. Specifically, we intend to analyse whether firms which (continue to) engage in work for the UK Government are systematically associated with greater abnormal returns than those firms which do not seek Cyber Essentials compliance to provide products or services to the Government.

Our future studies will also focus on the role of regulatory environments, IT maturity, and other country-level characteristics. Moreover, we aim to consider additional firm-level

characteristics such as different governance structures and the timing of investments relative to security breaches. Relatedly, we discuss multiple potential explanations of our results which should be tested empirically. Methodologically, future work could also include binomial/binary logistic regression models to examine variables influencing conditions under which cumulative abnormal returns tend to be negative. A separate study might also assess firms which choose not to re-certify and their respective reasons. Another way in which this current study can be extended is to assess long-term firm value and financial performance implications, given that event studies are only designed to measure short-term market reactions.

Acknowledgements

The authors would like to thank the anonymous reviewers for their constructive feedback.

References

[1] Russel Cameron Thomas, Marcin Antkiewicz, Patrick Florer, Suzanne Widup, and Matthew Woodyard. How Bad Is It? – A Branching Activity Model to Estimate the Impact of Information Security Breaches. In *Workshop on the Economics of Information Security (WEIS) 2013*, pages 1–34, 2013.

[2] Vilhelm Verendel. Quantified Security is a Weak Hypothesis: A Critical Survey of Results and Assumptions. In *Proceedings of the 2009 Workshop on New Security Paradigms*, pages 37–50, 2009.

[3] Ross Anderson, Chris Barton, Rainer Böhme, Richard Clayton, Michael J G van Eeten, Michael Levi, Tyler Moore, and Stefan Savage. Measuring the Cost of Cybercrime. In *Workshop on the Economics of Information Security (WEIS) 2012*, pages 1–31, 2012.

[4] Ponemon Institute. 2018 Cost of Data Breach Study, 2018.

[5] Sriram Somanchi and Rahul Telang. Impact of Security Events and Fraudulent Transactions on Customer Loyalty: A Field Study. In *Workshop on the Economics of Information Security (WEIS) 2017*, pages 1–16, 2017.

[6] Juhee Kwon and M Eric Johnson. The Market Effect of Healthcare Security: Do Patients Care about Data Breaches? In *Workshop on the Economics of Information Security (WEIS) 2015*, pages 1–34, 2015.

[7] Katherine Campbell, Lawrence A Gordon, Martin P Loeb, and Lei Zhou. The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market. *Journal of Computer Security*, 11(3):431–448, 2003.

[8] Anat Hovav and John D'Arcy. The Impact of Denial-of-service Attack Announcements on the Market Value of Firms. *Risk Management and Insurance Review*, 6(2):97–121, 2003.

[9] Huseyin Cavusoglu, Birendra Mishra, and Srinivasan Raghunathan. 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, 2004.

[10] Anat Hovav and John D'Arcy. The Impact of Virus Attack Announcements on the Market Value of Firms. *Information Systems Security*, 13(3):32–40, 2004.

[11] Karthik Kannan, Jackie Rees, and Sanjay Sridhar. Market Reactions to Information Security Breach Announcements: An Empirical Analysis. *International Journal of Electronic Commerce*, 12(1):69–91, 2007.

[12] Alvin Leung and Indranil Bose. Indirect Financial Loss of Phishing to Global Market. In *International Conference on Information Systems (ICIS) 2008*, pages 1–15, 2008.

[13] Sanjay Goel and Hany A Shawky. Estimating the Market Impact of Security Breach Announcements on Firm Values. *Information & Management*, 46(7):404–410, 2009.

[14] Edward A Morse, Vasant Raval, and John R Wingender. Market Price Effects of Data Security Breaches. *Information Security Journal: A Global Perspective*, 20(6):263–273, 2011.

[15] Ali Alper Yayla and Qing Hu. 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, 2011.

[16] Georgios Spanos and Lefteris Angelis. The Impact of Information Security Events to the Stock Market: A Systematic Literature Review. *Computers & Security*, 58:216–229, 2016.

[17] Sebastien Gay. Strategic News Bundling and Privacy Breach Disclosures. *Journal of Cybersecurity*, 3(2):91–108, 2017.

[18] Eli Amir, Shai Levi, and Tsafrir Livne. Do Firms Underreport Information on Cyber-attacks? Evidence from Capital Markets. *Review of Accounting Studies*, 23(3):1177–1206, 2018.

[19] Matthew P Barrett. Framework for Improving Critical Infrastructure Cybersecurity Version 1.1, 2018.

[20] Wing Man Wynne Lam. Attack-Deterring and Damage-Control Investments in Cybersecurity. In *Workshop on the Economics of Information Security (WEIS) 2015*, pages 1–24, 2015.

[21] Alfred Rappaport. *Creating Shareholder Value: The New Standard for Business Performance*. Free Press, New York, 1986.

[22] R Edward Freeman, Andrew C Wicks, and Bidhan Parmar. Stakeholder Theory and "the Corporate Objective Revisited". *Organization Science*, 15(3):364–369, 2004.

[23] Sangmi Chai, Minkyun Kim, and H Raghav Rao. Firms' Information Security Investment Decisions: Stock Market Evidence of Investors' Behavior. *Decision Support Systems*, 50(4):651–661, 2011.

[24] Rachel Rue, Shari Lawrence Pfleeger, and David Ortiz. A Framework for Classifying and Comparing Models of Cyber Security Investment to Support Policy and Decision-Making. In *Workshop on the Economics of Information Security (WEIS) 2007*, pages 1–23, 2007.

[25] Tyler Moore, Scott Dynes, and Frederick R Chang. Identifying How Firms Manage Cybersecurity Investment. In *Workshop on the Economics of Information Security (WEIS) 2016*, pages 1–27, 2016.

[26] United Kingdom Department for Culture Media and Sport; Ipsos MORI's Social Research Institute; University of Portsmouth. UK Cyber Security Breaches Survey 2017. 2017.

[27] Ross Anderson and Tyler Moore. The Economics of Information Security. *Science*, 314(5799):610–613, 2006.

[28] Tyler Moore and Ross Anderson. Economics and Internet Security: A Survey of Recent Analytical, Empirical, and Behavioral Research. *Harvard Computer Science Group Technical Report TR-03-11.*, pages 1–26, 2011.

[29] Rainer Böhme. Security Metrics and Security Investment Models. In Isao Echizen, Noboru Kunihiro, and Ryoichi Sasaki, editors, *Advances in Information and Computer Security*, pages 10–24, Berlin, 2010. Springer.

[30] Eva Weishäupl, Emrah Yasasin, and Guido Schryen. Information Security Investments: An Exploratory Multiple Case Study on Decision-making, Evaluation and Learning. *Computers & Security*, 77(August), 2018.

[31] Lawrence A Gordon and Martin P Loeb. The Economics of Information Security Investment. *ACM Transactions on Information and System Security (TISSEC)*, 5(4):438–457, 2002.

[32] Huseyin Cavusoglu, Birendra Mishra, and Srinivasan Raghunathan. A Model for Evaluating IT Security Investments. *Communications of the ACM*, 47(7):87–92, 2004.

[33] Eugene Francis Fama. Efficient Capital Markets: A Review of Theory and Empirical Work. *Journal of Finance*, 25(2):383–417, 1970.

[34] Eugene F Fama. Random Walks in Stock Market Prices. *Financial Analysts Journal*, 51(1):75–80, 1995.

[35] Rolf W Banz. The Relationship Between Return and Market Value of Common Stocks. *Journal of Financial Economics*, 9(1):3–18, 1981.

[36] Simon Benninga. *Financial Modeling*. MIT Press, Cambridge, MA, 4th ed edition, 2014.

[37] Stephen J Brown and Jerold B Warner. Using Daily Stock Returns: The Case of Event Studies. *Journal of Financial Economics*, 14(1):3–31, 1985.

[38] Stephen J Brown and Jerold B Warner. Measuring Security Price Performance. *Journal of Financial Economics*, 8(3):205–258, 1980.

[39] A Craig MacKinlay. Event Studies in Economics and Finance. *Journal of Economic Literature*, 35(1):13–39, 1997.

[40] Ross Anderson, Rainer Böhme, Richard Clayton, and Tyler Moore. Security Economics and European Policy. In *Workshop on the Economics of Information Security (WEIS) 2008*, pages 1–62, 2008.

[41] Rahul Telang and Sunil Wattal. Impact of Software Vulnerability Announcements on the Market Value of Software Vendors - An Empirical Investigation. In *Workshop on the Economics of Information Security (WEIS) 2005*, pages 1–34, 2005.

[42] Alessandro Acquisti, Allan Friedman, and Rahul Telang. Is There a Cost to Privacy Breaches? An Event Study. In *Workshop on the Economics of Information Security (WEIS) 2006*, pages 1–20, 2006.

[43] Brian L Dos Santos, Ken Peffers, and David C Mauer. The Impact of Information Technology Investment Announcements on the Market Value of the Firm. *Information Systems Research*, 4(1):1–23, 1993.

[44] Kun Shin Im, Kevin E Dow, and Varun Grover. A Reexamination of IT Investment and the Market Value of the Firm - An Event Study Methodology. *Information systems research*, 12(1):103–117, 2001.

[45] Debabroto Chatterjee, Carl Pacini, and V Sambamurthy. The Shareholder-Wealth and Trading-Volume Effects of Information-Technology Infrastructure Investments. *Journal of Management Information Systems*, 19(2):7–42, 2002.

[46] Bruce Dehning, Vernon J Richardson, and Robert W Zmud. The Value Relevance of Announcements of Transformational Information Technology Investments. *MIS Quarterly*, 27(4):637–656, 2003.

[47] Manish Agrawal, Rajiv Kishore, and H Raghav Rao. Market Reactions to e-business Outsourcing Announcements: An Event Study. *Information & Management*, 43(7):861–873, 2006.

[48] Vincent J Shea, Kevin E Dow, Alain Yee-Loong Chong, and Eric W T Ngai. An Examination of the Long-Term Business Value of Investments in Information Technology. *Information Systems Frontiers*, Online, 2017.

[49] Jason K Deane, David M Goldberg, Terry R Rakes, and Loren P Rees. The Effect of Information Security Certification Announcements on the Market Value of the Firm, 2019.

[50] Feng Xu, Xin (Robert) Luo, Hongyun Zhang, Shan Liu, and Wei (Wayne) Huang. Do Strategy and Timing in IT Security Investments Matter? An Empirical Investigation of the Alignment Effect. *Information Systems Frontiers*, Online, 2017.

[51] Indranil Bose and Alvin Chung Man Leung. The Impact of Adoption of Identity Theft Countermeasures on Firm Value. *Decision Support Systems*, 55(3):753–763, 2013.

[52] Srikanth Parameswaran, Srikanth Venkatesan, and Manish Gupta. Cloud Computing Security Announcements: Assessment of Investors' Reaction. *Journal of Information Privacy and Security*, 9(1):17–46, 2013.

[53] Christina Y Jeong, Sang-Yong Tom Lee, and Jee-Hae Lim. Information Security Breaches and IT Security Investments: Impacts on Competitors. *Information & Management*, In Press, 2018.

[54] Linda Brock and Yair Levy. The Market Value of Information System (IS) Security for e-banking. *Online Journal of Applied Knowledge Management*, 1(1):1–17, 2013.

[55] Eva Szubartowicz and Guido Schryen. Timing in Information Security: An Event Study on the Impact of Information Security Investment Announcements (Working Paper). Technical report, University of Regensburg, 2018.

[56] Juhee Kwon and M Eric Johnson. Proactive Versus Reactive Security Investments in the Healthcare Sector. *MIS Quarterly*, 38(2):451–471, jun 2014.

[57] Mukul Gupta, Alok R Chaturvedi, Shailendra Mehta, and Lorenzo Valeri. The Experimental Analysis of Information Security Management Issues for Online Financial Services. In *Proceedings of the 21st International Conference on Information Systems*, pages 667–675, 2000.

[58] Wei Liu, Hideyuki Tanaka, and Kanta Matsuura. An Empirical Analysis of Security Investment in Countermeasures Based on an Enterprise Survey in Japan. In *Workshop on the Economics of Information Security (WEIS) 2006*, pages 1–15, 2006.

[59] Daniel W Woods and Andrew C Simpson. Monte Carlo Methods to Investigate How Aggregated Cyber Insurance Claims Data Impacts Security Investments. *Workshop on the Economics of Information Security (WEIS) 2018*, pages 1–24, 2018.

[60] Chad Heitzenrater and Andrew C Simpson. Policy, Statistics, and Questions: Reflections on UK Cyber Security Disclosures. In *Workshop on the Economics of Information Security (WEIS) 2015*, pages 1–28, 2015.

[61] Claudia Biancotti. The Price of Cyber (In)security: Evidence from the Italian Private Sector. In *Workshop on the Economics of Information Security (WEIS) 2018*, pages 1–45. WEIS 2018, 2018.

[62] Elena Kvochko and Rajiv Pant. Why Data Breaches Don't Hurt Stock Prices, 2015.

[63] Joshua Danielson. Breaches Don't Correlate To Real Results, 2018.

[64] National Cyber Security Centre (NCSC). Cyber Essentials: Requirements for IT Infrastructure, 2018.

[65] National Cyber Security Centre (NCSC). Cyber Essentials: Getting Certified, 2018.

[66] Crown Commercial Service. Procurement Policy Note – Cyber Essentials Scheme, 2016.

[67] International Organization for Standardization. ISO/IEC 27000 Family - Information Security Management Systems, 2018.

[68] International Organization for Standardization. The ISO Survey of Management System Standard Certifications - 2017 - Explanatory Note, 2018.

[69] Wolfgang Böhmer. Appraisal of the Effectiveness and Efficiency of an Information Security Management System Based on ISO 27001. In *Emerging Security Information, Systems and Technologies, 2008. SECURWARE'08. Second International Conference on*, pages 224–231. IEEE, 2008.

[70] William F Sharpe. A Simplified Model for Portfolio Analysis. *Management Science*, 9(2):277–293, 1963.

[71] Harry Max Markowitz. Portfolio Selection. *Journal of Finance*, 7(1):77–91, 1952.

[72] William F Sharpe. Capital Asset Prices: A Theory of Market Equilibrium Under Conditions of Risk. *Journal of Finance*, 19(3):425–442, 1964.

[73] John Lintner. The Valuation of Risk Assets and the Selection of Risky Investments in Stock Portfolios and Capital Budgets. *Review of Economics and Statistics*, 47(1):13–37, 1965.

[74] Jack L Treynor. How to Rate Management of Investment Funds. *Harvard Business Review*, 43(1):63–75, 1965.

[75] Jan Mossin. Equilibrium in a Capital Asset Market. *Econometrica*, 34(4):768–783, 1966.

[76] Abagail McWilliams and Donald Siegel. Event Studies in Management Research: Theoretical and Empirical Issues. *Academy of Management Journal*, 40(3):626–657, 1997.

[77] Abagail McWilliams, Donald Siegel, and Siew Hong Teoh. Issues in the Use of the Event Study Methodology: A Critical Analysis of Corporate Social Responsibility Studies. *Organizational Research Methods*, 2(4):340–365, 1999.

[78] John Hughes, Jing Liu, and Jun Liu. Information Asymmetry, Diversification, and Cost of Capital. *The Accounting Review*, 82(3):705–729, 2006.

[79] Frank Wilcoxon. Individual Comparisons by Ranking Methods. *Biometrics Bulletin*, 1(6):80–83, 1945.

[80] Joseph L Jr Hodges and Erich L Lehmann. Estimates of Location Based on Rank Tests. *Annals of Mathematical Statistics*, pages 598–611, 1963.

[81] Hyun-Chul Cho and Shuzo Abe. Is Two-Tailed Testing for Directional Research Hypotheses Tests Legitimate? *Journal of Business Research*, 66(9):1261–1266, 2013.

[82] Cabinet Office. Press release: Government mandates new cyber security standard for suppliers, 2014.