

# The Impact of CISO Appointment Announcements on the Market Value of Firms

Adrian Ford<sup>1</sup>, Ameer Al-Nemrat<sup>1</sup>, Seyed Ali Ghorashi<sup>1</sup> and Julia Davidson<sup>2</sup>

<sup>1</sup>School of Architecture, Computing and Engineering, University of East London, UK

<sup>2</sup>Royal Docks School of Business and Law, University of East London, UK

[a.ford1701@uel.ac.uk](mailto:a.ford1701@uel.ac.uk)

**Abstract:** Previous studies concerning the economic impact of security events on publicly listed companies have focussed on the negative effect of data breaches and cyberattacks with a view to encouraging firms to improve their cyber security posture to avoid such incidents. This paper is an initial study on the impact of investment in human capital related to security, specifically appointments of chief information security officers (CISO), chief security officers (CSO) or similar overall head of security roles. Using event study techniques, a dataset of 37 CISO type appointment announcements spanning multiple world markets between 2012 and 2019 was analysed and statistically significant (at the 5% level) positive cumulative abnormal returns (CAR) of around 0.8% on average were observed over the three-day period before, during and after the announcement. Furthermore, this positive CAR was found to be highest, at nearly 1.8% on average, within the financial services sector and showing statistical significance at the 1% level. In addition to the industry sector, other characteristics were investigated such as job title, reporting structure, comparison of internal versus external appointments, gender and variations between markets. Although these findings were not as conclusive they are, nevertheless, good pointers for future research in this area. This overall positive market reaction to CISO related announcements is a strong case for publicly listed firms to be transparent in such appointments and to, perhaps, review where that function sits within their organisation to ensure it delivers the greatest benefits. As 24% of the firms analysed were listed outside the US, this study also begins to counter the strong US bias seen in similar and related studies. This research is expected to be of interest to business management, cyber security practitioners, investors and shareholders as well as researchers in cyber security or related fields.

**Keywords:** cyber security, CISO, CSO, market value, economic impact, event study

## 1. Introduction

The US Federal Bureau of Investigation (IC3 2020) reported a 69% increase in internet crime related complaints from 2019. With cybercrime so rife, along with damaging high-profile data breaches such as that of Marriott and British Airways (Ford et al. 2021a), cyber security should be very much a concern for organisations globally. Indeed, the UK Department for Digital Culture, Media and Sport report that 77% of businesses view cyber security as a high priority at board level (DCMS 2021) and Gartner (2021) predict that by 2025, 40% of boards will have cyber security committees established and overseen by a “*suitably qualified*” executive. Therefore, given the importance of cyber security, in the case of publicly listed companies one could reasonably expect markets to react in a positive way to news of investment in this area. This study is concerned with announcements of investment in human capital, specifically heads of security at executive level such as chief information security officer (CISO), chief security officer (CSO) or similar roles<sup>1</sup>, the primary research question being what is the impact (if any) of this information on the market value of firms? The ability to measure and clearly identify any positive impact would surely encourage organisations to both invest in, as well as publicise establishment or improvement of their security functions and thereby their overall cyber security posture<sup>2</sup>. Existing literature relating specifically to CISOs is rather sparse (Karanja & Rosso 2017) so this small scale initial study would also begin to fill a knowledge gap. Such research is expected to be of interest to business management, cyber security practitioners, investors and shareholders as well as researchers in cyber security or related fields.

## 2. Related work

Looking elsewhere, due to the dearth of literature on CISOs as reported by Karanja and Rosso (2017), Chatterjee, Richardson and Zmud (2001) examined the economic impact of the creation of new chief information officer (CIO) positions using event study techniques and observed positive market reactions of 1.16% on average and even higher (almost 3%) for heavily information technology (IT) driven industry sectors. This variation between sectors was also reported by Tweneboah-Kodua, Atsu and Buchanan (2018) who observed that financial services firms reacted more rapidly and more significantly than those in the technology sector. Their study focussed on

<sup>1</sup>For convenience, hereinafter the acronym ‘CISO’ will be used as a generic term to refer to roles of this type.

<sup>2</sup>Cyber security posture is a term encompassing training and awareness in addition to governance and technical solutions.

the negative impact of cyberattacks on stock returns and a systematic literature review by Spanos and Angelis (2016) found that 76% of studies in this area reported an impact which was both negative and statistically significant. For instance, Lin et al. (2020) observed losses of 1.44% on average over a five-day window. Andoh-Baidoo, Amoako-Gyampah and Osei-Bryson (2010) found -3.18% abnormal returns over a three-day period. Cavusoglu, Mishra and Raghunathan (2004) observe -2.1% on average over the two days following the announcement. Goel and Shawky (2009) cite -1% in the days immediately surrounding the event.

Moving back to positive economic impacts, literature in this area was found to be lacking. Cavusoglu et al. (2004) found a positive impact on security developers after the disclosure of security breaches by affected firms. Deane et al. (2019) studied ISO 27001 certification announcements and found the abnormal market returns both positive and statistically significant (0.72% on average over two days). A more recent systematic literature review (Ali et al. 2021) updating the work of Spanos and Angelis (2016) acknowledges the relative lack of studies concerning the positive impact of favourable information security events such as regulation, certification or investment also noting that such favourable events generate lower magnitude abnormal returns (in the range 0.63% to 1.36%) than unfavourable events which could lose up to 10% of market value.

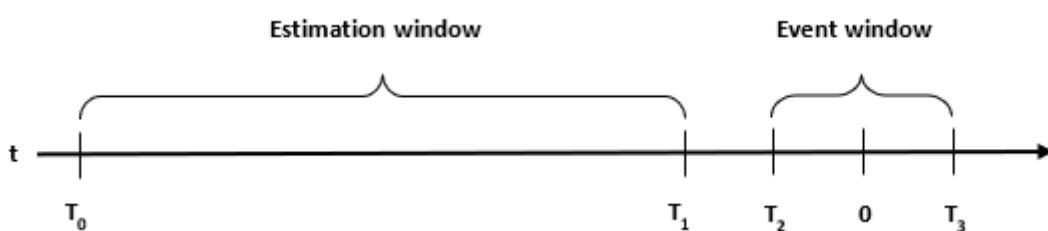
This study, therefore, will not only increase the CISO research knowledgebase but also help address the shortfall in studies on favourable security events. Ali et al. (2021) also note that 76% of existing similar studies were based solely on US data, so the aim here was also to look globally as far as possible (given English language restrictions) in an attempt to offset this US bias (cf. Ford et al. 2021b).

### 3. Methodology

From a high-level perspective, the approach to this research was first, to hand gather a dataset of CISO appointment announcements, then filter this dataset keeping only those examples related to publicly listed companies. The final step was to identify any impact of these announcements on the share price of each firm through event study techniques.

#### 3.1 Event studies

Event studies are a widely reported method to assess the impact of a specific event on the share price (market value) of firms - a detailed description may be found in e.g. MacKinlay (1997). A key assumption of this method is the ability of the market to reflect all available information as described by the efficient market hypothesis (i.a. Fama 1970). Through the observation of share price movements in reaction to information regarding a specific event, such as an executive appointment announcement, over a short time period (the event window), it is possible to ascertain how the market reacted to that specific event, with the caveat of no other confounding events occurring during this period.



**Figure 1:** Event study timeline

A frequently used approach for information security related event studies is the market model (e.g. Cavusoglu et al. 2004; Andoh-Baidoo et al. 2010; Hinz et al. 2015; Schatz & Bashroush 2016; Castillo & Falzon 2018; Tweneboah-Kodua et al. 2018; Jeong et al. 2019; Ford et al. 2021a,b) which, through a regression analysis of a firm's share price over a relatively long estimation window (see **Figure 1**), is able to predict stock returns during the later (usually much shorter) event window. This approach assumes that returns follow a single factor model (1) where the return of firm  $i$  on day  $t$  ( $R_{i,t}$ ) is dependent on the corresponding daily return of the reference market ( $R_{m,t}$ ) and the extent of the security's responsiveness ( $\beta_i$ ) offset by its abnormal return ( $\alpha_i$ ). The error term  $\varepsilon_{i,t}$  is expected to be zero with finite variance. Abnormal returns are calculated for the event window (2) and reported as a cumulative abnormal return (CAR) over the whole event window (3). For cross-sectional analyses, a cumulative average abnormal return (CAAR) was calculated over  $N$  events (4).

$$R_{i,t} = \alpha_i + \beta_i \cdot R_{m,t} + \varepsilon_{i,t} \quad (1)$$

$$AR_{i,t} = R_{i,t} - (\alpha_i + \beta_i \cdot R_{m,t}) \quad (2)$$

$$CAR_i = \sum_{t=T_2}^{T_3} AR_{i,t} \quad (3)$$

$$CAAR = \frac{1}{N} \sum_{i=1}^N CAR_i \quad (4)$$

### 3.2 Data collection

The base dataset was hand-gathered from internet searches for CISO appointments<sup>3</sup> building up a Microsoft Excel spreadsheet. Many results were clearly governmental organisations or not-for-profits or private companies, so were discarded. It was decided to cap the date range at 31/12/2019 in order to avoid market uncertainties due to COVID-19, that in itself being a long-term confounding event. Once the residual set seemed to be mostly publicly listed companies each data record was carefully reviewed, ensuring that the stock was still listed and share price data available. Data fields extracted included company name, announcement date, job title, position in the organisation (reporting line) and gender. Some announcements made it clear this was a newly created CISO position and so these were marked as such whereas others merely implied this – these were flagged separately due to the lesser information salience (e.g. Ramos, Latoeiro & Veiga 2020). Other records had to be filtered out as they were not listed before the start of the estimation window. A few examples (Bridgestone Americas, Santander UK and CareerBuilder) were related to subsidiary companies but these were kept as there would be a contribution, at least, to any market reaction despite less salience, also to maintain as large a dataset as possible. Once the filtering was complete, a dataset of 41 records remained. The final step was to look for confounding events. The dates of the nearest events (before/after day zero) were also recorded so these could be filtered out dynamically as needed. Confounding events were considered to be earnings/dividend announcements or another executive appointment (consistent with e.g. Chatterjee et al. 2001). There were three examples (Digital Realty, Wells Fargo, Axon) where joint announcements were made with other positions and these were included, again to maximise the dataset despite the lesser salience.

The importance of the choice of market index to use as a reference has been highlighted by e.g. Kannan, Rees and Sridhar (2007). Consistent with Ford et al. (2021b), the most appropriate market index was chosen in each case being, ideally, one in which the stock in question was included and favouring narrower, more focussed indices rather than a one-size-fits-all approach given, of course, that this index data was available from Yahoo!Finance (otherwise the next best was selected). Some firms had multiple listings, in which case the primary listing and associated index were used.

### 3.3 Data analysis

To facilitate the analyses, R (R Core Team 2018)<sup>4</sup> code was developed to extract share price and index data directly from Yahoo!Finance for each data record. Event studies were then carried out through an R package (Schimmer, Levchenko & Müller 2014)<sup>5</sup> applying the market model as described above. Announcements falling on non-trading days were defaulted to the next available trading day. An estimation window of 120 days was chosen, consistent with previous studies (e.g. Goel & Shawky 2009; Andoh-Baidoo et al. 2010; Schatz & Bashroush 2016; Richardson et al. 2019) ending one trading day before the event window in all cases. Tweneboah-Kodua et al. (2018) recommend avoiding overlap of the estimation and event windows in this way to avoid “parameter contamination”. Although the event window should be broad enough to contain any uncertainty in the date of the event, the longer the window, the less likely it is to detect abnormal returns (Dyckman, Philbrick, & Stephan 1984). Some studies observed a market reaction in advance of the event date due to information leakage, such as Lin et al. (2020) who found significant evidence of opportunistic pre-official announcement insider trading related to data breaches using event studies. For this exercise, a range of event windows were initially chosen starting from up to two days before the event and varying in length from 2 up to 20 trading days to catch any pre-event effects as well as others, for instance, sector specific effects reported by

<sup>3</sup> Sources included ProQuest (CSO Online), Google and Bing

<sup>4</sup> R version 4.1.2 (2021-11-01)

<sup>5</sup> EventStudy package version 0.36.900 (API version 1.059)

i.a. Tweneboah-Kodua et al. (2018) who observed more rapid responses to information security events from e.g. the financial services sector thereby justifying longer event windows for sectorial comparison purposes.

### 3.4 Hypothesis development

The null hypothesis for event studies maintains that there are no abnormal returns within the event window. The standard deviation of abnormal returns during the event window is described by (5) where  $M_i$  refers to the number of non-missing returns. The t-value for the CAR over the event window for each firm  $i$  was then calculated according to (6).

$$S_{AR_i} = \sqrt{\frac{1}{M_i - 2} \sum_{t=T_0}^{T_1} (AR_{i,t})^2} \quad (5)$$

$$t_{CAR_i} = \frac{CAR_i}{\sqrt{(T_3 - T_2 + 1) S_{AR_i}^2}} \quad (6)$$

For cross-sectional analyses the t-statistic ( $t_{CAAR}$ ) was calculated based on the CAAR (8) with  $S_{CAAR}$  being the standard deviation of the CARs for each firm  $i$  across the sample of size  $N$ (7).

$$S_{CAAR} = \sqrt{\frac{1}{N - 1} \sum_{i=1}^N (CAR_i - CAAR)^2} \quad (7)$$

$$t_{CAAR} = \sqrt{N} \frac{CAAR}{S_{CAAR}} \quad (8)$$

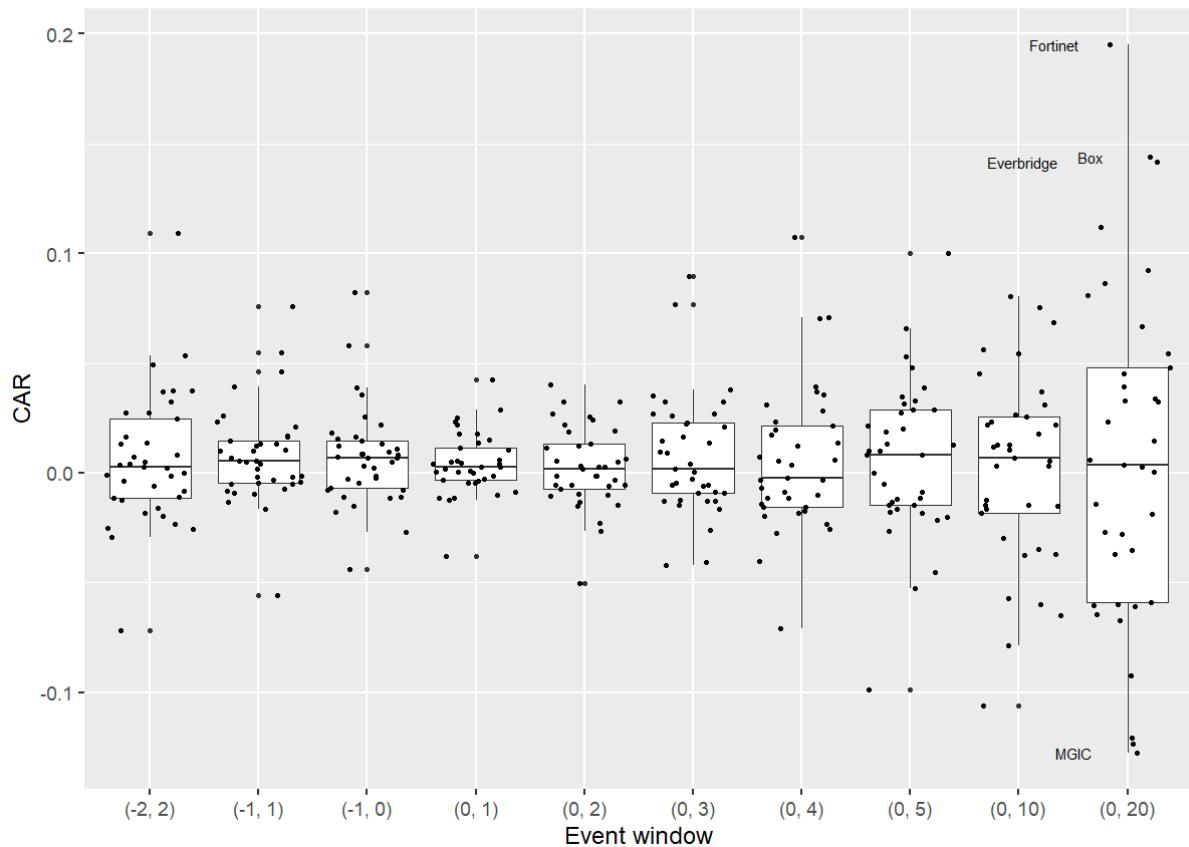
Significance testing in this way is consistent with e.g. Castillo and Falzon (2018), Deane et al. (2019) and Jeong et al. (2019). Indeed, Deane et al. (2019: 115) argue that “*the t test is considered to be the best framework for analyzing statistical significance in most event study frameworks and to be relatively robust*”.

## 4. Results and discussion

Event studies were carried out as above for 10 event windows of differing length across all 41 CISO appointment announcements. A visualisation of the overall results showed that event windows (-1, 1) and (-1, 0) were of interest and thus records with confounding events  $\pm 2$  days were filtered out<sup>6</sup> leaving 37 records. The revised visualisation is shown in **Figure 2**. The most positive impact is seen around the three or two-day event windows (-1, 1), (-1, 0) with the market value reverting back to normal by day 4. There was also a slight peak at day 5, but of course, this may be due to confounding events. By day 20 it can be seen that Fortinet is the best performing stock with a CAR of almost 20%, and MGIC the worst.

---

<sup>6</sup>This is a quite stringent approach, similar studies have only filtered out confounding events within the event window, this approach leaves a gap of one day in case of any advance information leakage of the confounding event.



**Figure 2:** Comparison of event windows

A CAAR was calculated for multiple firms across each window and the results shown in **Table 1**. The three-day event window (-1, 1) showed the most positive CAAR of almost 0.8% (significant at the 5% level), similar to the findings of e.g. Chatterjee et al. (2001) for CIO appointments with their dataset being of a comparable size as well (1.16% over 96 announcements). The fact that this includes a pre-event day indicates a little information leakage prior, as the date accuracy was carefully verified (cf. Lin et al. 2020). Within this window, 22 of the 37 events (59%) had abnormal returns of greater than zero, therefore this window was chosen as the basis for further analyses. Usage of this event window (-1, 1) has been previously reported in studies of this type (e.g. Chatterjee et al. 2001; Andoh-Baidoo et al. 2010; Bose & Leung 2014; Khansa 2015; Modi et al. 2015). A lack of statistical significance for the longer windows is also seen, indicative of a tendency of market recovery towards zero abnormal returns over time as reported by Dyckman et al. (1984).

**Table 1:** CAAR by event window

Event Window	N	CAAR	t <sub>CAAR</sub>	% Positive CAR
(-2, 2)	37	0.0062	1.2356	54
(-1, 1)	37	0.0077	2.1091**	59
(-1, 0)	37	0.0070	1.8997*	62
(0, 1)	37	0.0043	1.8334*	65
(0, 2)	37	0.0025	0.8411	51
(0, 3)	37	0.0075	1.6717	54
(0, 4)	37	0.0055	1.0091	49
(0, 5)	37	0.0059	1.0054	57
(0, 10)	37	0.0015	0.2074	59
(0, 20)	37	0.0070	0.5529	57
	<b>370</b>	<b>0.0055</b>		<b>57</b>

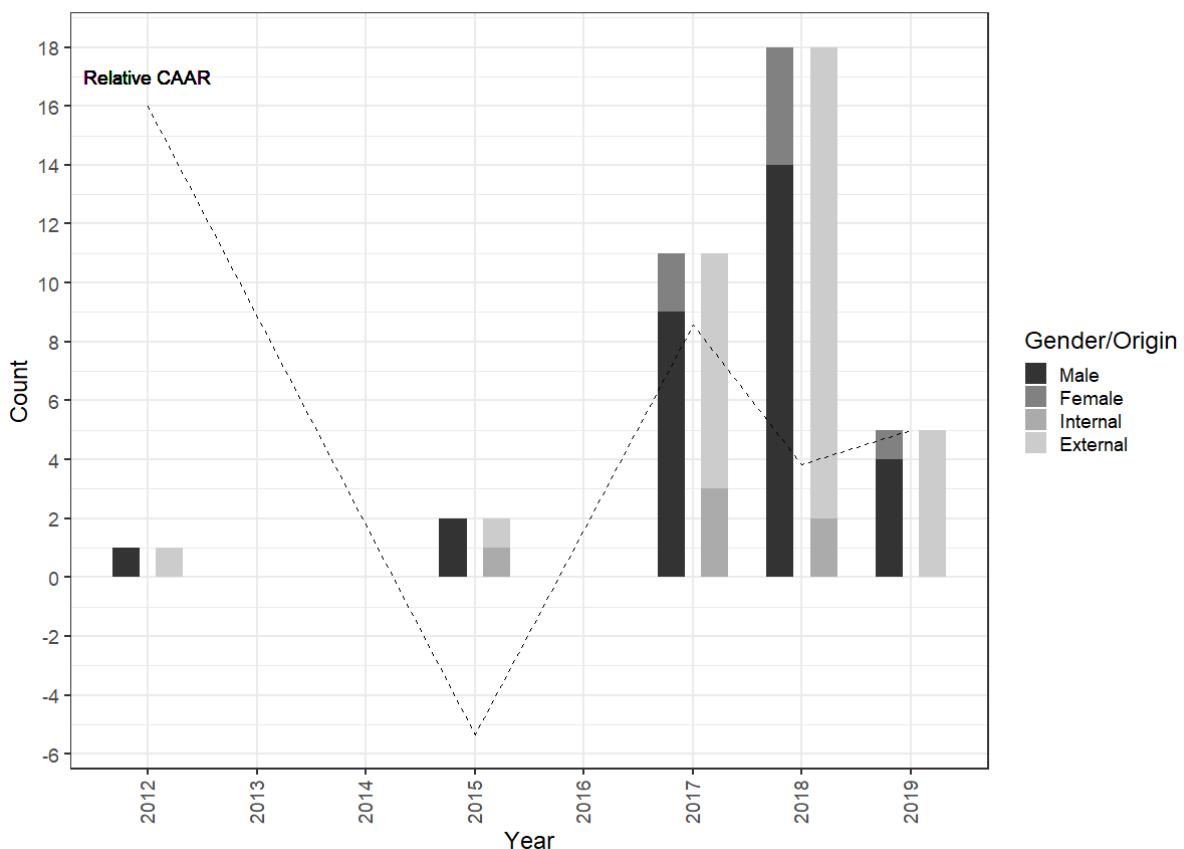
\*,\*\*,\*\*\* Represent statistical significance at the 10%, 5% and 1% levels respectively.

A visualisation of how the data changes over time is shown in **Figure 3**. Out of the 37 total events in the dataset, by far the majority (92%) occurred between 2017 and 2019 but the overall number of CISO announcements does

not seem to be increasing year-on-year - it actually dropped from 18 to 5 in the last two years sampled, so there seems to be a lack of awareness of the potential benefits of sharing this information with the market. A relative measure of the CAAR is also shown flipping from positive in 2012 to negative in 2015 and remaining positive for the bulk of the dataset in the final three years.

Regarding the origin of the appointment, internal appointments were low (27%) in 2017 dropping to 11% in 2018 and subsequently to zero in 2019. So, if we ignore the sparse data in previous years we have a trend toward solely external recruitment. Interestingly the internal appointments, although less at 6 out of 37 (16%), generated a CAAR of 1.28% which was almost double that of the way more frequent external appointments (CAAR=0.67%) although these results were not statistically significant. Chatterjee et al. (2001) suggest that the market may respond better to internal appointments because the appointee would 'hit the ground running' due to existing in-depth knowledge of the business and established relationships with management.

Karanja and Rosso (2017) observed in their dataset of 55 CISOs spanning 2010-2014 that only 11% were female. Although here it is difficult to identify any clear trend over time, it can be noted there were no such examples in the data sample prior to 2017 (although only three data points) yet in the final three years the percentage of women was fairly constant (18, 22, 20%) so despite the lack of any obvious trend in the data here, comparing with Karanja and Rosso (2017) we see almost double the percentage of women CISOs – a refreshing increase in diversity. That said, the 30 examples (82%) of male appointees yielded a CAAR of +0.85% significant at the 5% level whereas the remaining 7 female appointments generated only +0.38% which was, unfortunately, not statistically significant.



**Figure 3:** Breakdown by year

A breakdown of CAAR by sector is shown in **Table 3**. The financial services sector was the clear winner showing positive CARs of almost 1.8% on average and statistical significance at the 1% level. Such sector specific behaviour has been highlighted in e.g. Tweneboah-Kodua et al. (2018). It is interesting to note that 17 out of 37 announcements sampled (46%) belonged to this sector perhaps indicating more willingness (or regulation, of course) for transparency within this industry. It does seem surprising that negative market sentiment was

identified for 10 examples spanning 4 sectors especially one as sensitive as communication services which came in at more than 1% negative. Nevertheless, there is a deficiency of data here and no statistical significance.

**Table 2:** CAAR by industry sector

Industry Sector	N	CAAR	t <sub>CAAR</sub>	% Positive CAR
Financial Services	17	0.0178	3.3027***	76
Healthcare	1	0.0169		100
Consumer Cyclical	2	0.0077	3.2553	100
Utilities	1	0.0066		100
Technology	6	0.0046	0.5974	50
Real Estate	1	-0.0047		0
Consumer Defensive	1	-0.0082		0
Industrials	5	-0.0084	-0.6592	40
Communication Services	3	-0.0101	-2.8456	0
	<b>37</b>	<b>0.0077</b>		<b>59</b>

\*\*\*,\*\*\* Represent statistical significance at the 10%, 5% and 1% levels respectively.

Looking more closely at the content of the announcements, information on job title and position in the organisation are shown in **Table 4** and **Table 5** respectively. The most positive returns seem to occur when the CISO title is combined with a VP/SVP position – clearly this is recognised by the market as having more influence within the organisation although due to lack of data it is not statistically significant. The title CSO (a broader role not restricted to only information security) does show some significance but only at the 10% level. Even the single example of appointment of a Deputy CISO role (occurring shortly after the CISO was recruited) showed positive CAR at nearly 0.5%. Interestingly, combination of the security role with the CIO title results in the least positive CAR, or with that of trust (CTSO) yields negative of 1.7%. It appears that the market is preferring a focussed role with a high level of influence.

**Table 3:** CAAR by job title

Title	N	CAAR	t <sub>CAAR</sub>	% Positive CAR
VP/CISO	3	0.0358	2.4170	100
SVP/CISO	1	0.0234		100
CSO	6	0.0098	2.0353*	83
Global Head of Cyber Risk	1	0.0053		100
Deputy CISO	1	0.0048		100
CISO	23	0.0043	0.8788	43
CIO/CISO	1	0.0017		100
CTSO	1	-0.0165		0
	<b>37</b>	<b>0.0077</b>		<b>59</b>

\*\*\*,\*\*\* Represent statistical significance at the 10%, 5% and 1% levels respectively.

Carrying forward the argument of influence we can get some idea of the position in the organisation from some (16 out of 37 were not specified)<sup>7</sup> of the announcements where the reporting line was cited in **Table 5**. First of all, the results where data were available were not significant, so the null hypothesis cannot be rejected, although it is interesting to note that the expected result of direct CEO reporting (and therefore greatest influence) being the highest CAAR is not the case - it seems that COO or CFO reporting is more well received by the market. If the concept of operations is combined with technology (CTO) or EVP though, the result is negative! The observation that a reporting line into the CIO yields negative CAAR seems consistent with Williams (2007) and the conflict of interest argument – would there be reluctance on the part of such a CISO to call out security flaws in the CIO's IT environment?

**Table 4:** CAAR by CISO reporting line

Reporting line	N	CAAR	t <sub>CAAR</sub>	% Positive CAR
COO	2	0.0215	0.8737	50
CFO	1	0.0162		100
CEO	4	0.0148	1.3565	75
Corporate Secretary	1	0.0134		100
CTO	1	0.0130		100

<sup>7</sup> In some cases, it could be assumed from the announcement, however unless explicit it was classified as unspecified.

Reporting line	N	CAAR	t <sub>CAAR</sub>	% Positive CAR
(not specified)	16	0.0107	1.7592*	62
CISO	1	0.0048		100
CTO/COO	1	-0.0013		0
CIO	8	-0.0033	-0.3978	50
EVP Operations	1	-0.0047		0
SVP	1	-0.0050		0
	37	0.0077		59

\*,\*\*,\*\*\* Represent statistical significance at the 10%, 5% and 1% levels respectively.

The Chatterjee et al. (2001) study was restricted to the establishment of newly created CIO positions only. If the CISO announcements here contained a clear or implied indication that this was a new CISO position this was captured in the data record and analysed as shown in **Table 6**. The results were almost the exact opposite of expected, that the market would react better if an organisation was currently lacking an established security function. Perhaps the market expectation is that there should already be such a function in existence? The results are not significant except those cases where new or established was not specified which was a clear positive CAAR approaching 1.2%.

**Table 5:** Analysis of new or established CISO roles

New or established?	N	CAAR	t <sub>CAAR</sub>	% Positive CAR
(not specified)	25	0.0115	2.6205**	64
New (implied)	4	0.0015	0.2505	50
New (specified)	8	-0.0013	-0.1501	50
	37	0.0077		59

\*,\*\*,\*\*\* Represent statistical significance at the 10%, 5% and 1% levels respectively.

In view of the intended international nature of this study, an analysis by different markets is shown in **Table 7** using market currency as a primary key (to be less granular due to data deficiency). Here India shows by far the highest CAR of over 7.6% but with only one example. It is the UK and US who show significantly positive CAARs at the 5% level (with the UK almost double that of the US). Only Israel and Australia are displaying negative CAARs, but again lacking data. Despite no intended US focus, we see that 28 out of 37 (76%) announcements originated from US markets so there is little opportunity to analyse other markets in detail. This percentage matches closely the observation of Ali et al. (2021) on US dominance in such research who attribute this to regulatory effects encouraging transparency in addition to language restrictions. Over time there is an expectation that transparency (and thus availability of data) will increase in other markets as new regulations come into force.

**Table 6:** Analysis by market currency

Market Currency	N	CAAR	t <sub>CAAR</sub>	% Positive CAR
INR	1	0.0757		100
GBP	2	0.0158	14.3636**	100
USD	28	0.0081	2.4346**	61
JPY	1	0.0053		100
EUR	2	0.0052	0.6242	50
ILS	1	-0.0013		0
AUD	2	-0.0320	-1.3453	0
	37	0.0077		59

\*,\*\*,\*\*\* Represent statistical significance at the 10%, 5% and 1% levels respectively.

## 5. Conclusion

It has been shown in this introductory study that the announcement by a publicly listed company of a CISO appointment does indeed induce a positive market reaction, particularly within the financial services sector (+1.8% in the three days surrounding the event). In the data sample of 37 announcements analysed, 17 were financial services companies indicating a sector specific willingness to report, or regulatory effect.

Based on our analyses, we would advise the following content for a CISO appointment announcement to deliver maximum positive abnormal market return (ideally the hiring organisation would be a US or UK listed company in the financial services sector): job title CISO with VP or SVP responsibility stipulated (no mention whether this

is a new or established role), internal placement, male, reporting to the COO, CFO, or CEO but definitely not the CIO!

Chatterjee et al. (2001) calculated an approximate range of US\$7.5m (median approach) to US\$76m (mean approach) increase in market capitalisation for CIO appointments thereby easily justifying "*the trend in escalated executive salaries*"! Repeating this estimation across this whole CISO dataset gives a range of US\$94m to US\$318m, so it seems that this trend is very much continuing and clearly applies to CISOs as well!

This research should highlight the clear economic benefit of CISO appointments, as well the advantage of transparency in this area, to business management through the value the market places on the CISO role. There is an opportunity for other sectors to follow the lead of financial services and for other markets to adopt US practices and get ahead of the curve before new regulations come into effect. Once more data becomes available this exercise could be revisited for more in-depth analyses.

## **Acknowledgements**

The authors wish to thank the anonymous reviewer for their helpful comments in improving this manuscript.

## **References**

- Ali, S.E.A., Lai, F.-W., Dominic, P.D.D., Brown, N., Lowry, P.B., Ali, R.F. (2021), *Stock market reactions to favorable and unfavorable information security events: A systematic literature review*, Computers & Security, **110**, 102451
- Andoh-Baidoo F.K., Amoako-Gyampah K., Osei-Bryson K.M. (2010), *How Internet security breaches harm market value*, IEEE Security and Privacy **8**(1), 36–42
- Bose, I., Leung, A.C.M. (2014), *Do phishing alerts impact global corporations? A firm value analysis*, Decision Support Systems, **64**, 67–78
- Cavusoglu, H., Mishra, B., Raghunathan, S. (2004), *The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers*, International Journal of Electronic Commerce, **9**, 69-104
- Chatterjee, D., Richardson V.J., Zmud, R.W. (2001), *Examining the Shareholder Wealth Effects of Announcements of Newly Created CIO positions*, MIS Quarterly, **25**(1), 43-70, <https://www.jstor.org/stable/3250958>
- DCMS (2021), *Cyber Security Breaches Survey 2021*, <https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021/cyber-security-breaches-survey-2021>
- Deane J.K., Goldberg D.M., Rakes T.R., Rees L.P. (2019), *The effect of information security certification announcements on the market value of the firm*. Information Technology & Management, **20**(3), 107-121
- Dyckman, T., Philbrick, D., Stephan, J. (1984), *A Comparison of Event Study Methodologies Using Daily Stock Returns: A Simulation Approach*, Journal of Accounting Research, **22**, (Supplement)
- Fama, E. F. (1970), *Efficient Capital Markets: A Review of Theory and Empirical Work*, The Journal of Finance, **25**(2), 383–417
- Ford, A., Al-Nemrat, A., Ghorashi, S., Davidson, J. (2021a), *The Impact of GDPR Infringement Fines on the Market Value of Firms*, Proceedings of the 20th European Conference on Cyber Warfare and Security, <https://doi.org/10.34190/EWS.21.088>
- Ford, A., Al-Nemrat, A., Ghorashi, S., Davidson, J. (2021b), *The Impact of Data Breach Announcements on Company Value in European Markets*, WEIS 2021: The 20th Annual Workshop on the Economics of Information Security, <https://weis2021.econinfosec.org/wp-content/uploads/sites/9/2021/06/weis21-ford.pdf>. Accessed on: 21/12/2021
- Gartner Inc. (2021), *Gartner Predicts 40% of Boards Will Have a Dedicated Cybersecurity Committee by 2025*, <https://www.gartner.com/en/newsroom/press-releases/2021-01-28-gartner-predicts-40--of-boards-will-have-a-dedicated->
- Goel, S., Shawky, H.A. (2009), *Estimating the market impact of security breach announcements on firm values*, Information & Management, **46**(7), 404-410
- Hinz, O., Nofer, M., Schiereck, D., Trillig, J. (2015) *The influence of data theft on the share prices and systematic risk of consumer electronics companies*, Information & Management, **52**(3), 337-347
- IC3 - Internet Crime Complaint Center (2020), *Internet Crime Report 2020*, [https://www.ic3.gov/Media/PDF/AnnualReport/2020\\_IC3Report.pdf](https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf)
- Jeong, C., Lee, S., Lim, J. (2019), *Information security breaches and IT security investments: Impacts on competitors*, Information & Management, **56**(5), 681-695
- Kannan, K., Rees, J., Sridhar, S., (2007), *Market Reactions to Information Security Breach Announcements: An Empirical Analysis*, International Journal of Electronic Commerce, 01 September **12**(1), 69-91
- Lin, Z., Sapp, T.R., Ulmer, J.R., Parsa, R. (2020) *Insider trading ahead of cyber breach announcements*, Journal of Financial Markets, **50**, 100527
- Karanja, E., Rosso, M.A. (2017), *The Chief Information Security Officer: An Exploratory Study*, Journal of International Technology and Information Management, **26**(2), 23-47

- Khansa L. (2015), *M&As and market value creation in the information security industry*, *Journal of Economics and Business*, **82**, 113–134
- Ramos S.B., Latoeiro P., Veiga, H. (2020), *Limited attention, salience of information and stock market activity*, *Economic Modelling*, **87**, 92-108
- MacKinlay, A. C. (1997), *Event Studies in Economics and Finance*, *Journal of Economic Literature* **35**(1) (March)
- Modi, S.B., Wiles, M.A., Mishra, S. (2015), *Shareholder value implications of service failures in triads: The case of customer information security breaches*, *Journal of Operations Management*, **35**, 21–39
- R Core Team (2018), *R: A language and environment for statistical computing*. R Foundation for Statistical Computing, Vienna, Austria. Available on: <https://www.R-project.org/>
- Richardson, V.J., Smith, R.E, Watson, M.W. (2019) *Much Ado about Nothing: The (Lack of) Economic Impact of Data Privacy Breaches*, *Journal of Information Systems*: **33**(3), 227-265
- Schatz, D., Bashroush, R. (2016), *The impact of repeated data breach events on organisations' market value*, *Information & Computer Security*, **24**(1), 73-92
- Schimmer, M., Levchenko, A., and Müller, S. (2014), *EventStudyTools (Research Apps)*, St.Gallen. Available on: <http://www.eventstudytools.com>. Accessed on: 26/02/2021
- Spanos, G., Angelis, L. (2016), *The impact of information security events to the stock market: A systematic literature review*, *Computers and Security*, **58**, 216-229
- Tweneboah-Kodua, S., Atsu, F. and Buchanan, W. (2018), *Impact of cyberattacks on stock performance: a comparative study*, *Information and Computer Security*, **26**(5), 637-652
- Williams, P. (2007), *Executive and board roles in information security*, *Network Security*, **8**, 11-14
- Yahoo!Finance (2019), *Historical Data*, <https://finance.yahoo.com/quote>