The Impact of Data Breach Announcements on Company Value in European Markets

Adrian Ford[1], Ameer Al-Nemrat[1], Seyed Ali Ghorashi[1] and Julia Davidson[2]
[1]School of Architecture, Computing and Engineering
[2]Royal Docks School of Business and Law
University of East London
London, United Kingdom
{a.ford1701}@uel.ac.uk

Abstract—**Recent research on the economic impact of data breach announcements on publicly listed companies was found to be sparse, with the majority of existing studies having a strong US bias. Here, a dataset of 45 data breach disclosures between 2017 and 2019 relevant to European publicly listed companies was hand-gathered (from various sources) and detailed analyses of share price impact carried out using event study techniques with the aim of supporting business cases for firms to invest in cyber security. Differences from existing studies (in particular, the US market) are highlighted and discussed along with pointers to future research in this area. Although some evidence of negative cumulative abnormal returns (CAR) in the days surrounding the announcement were observed, along with one extreme case leading to insolvency, the results were not statistically significant overall with the notable exception of the Spanish market, which appeared to be more sensitive to data breaches, reacting rapidly. Therefore, justification for cyber security investment purely based on the market value effect of a data breach disclosure would be challenging. Other factors would need to be taken into consideration such as risk appetite, industry sector and nature of the information compromised as well as relevant legislation. Certain other observations were noted such as the lack of a comprehensive breach database for Europe (unlike US) and the effect of the introduction of the General Data Protection Regulation (GDPR). This research would be of benefit to business management, practitioners of cyber security, investors and shareholders as well as researchers in cyber security or related fields.**

Keywords—cyber security, data breaches, event study, market value, economic impact.

I. INTRODUCTION

A. Research Background

The Cyber Security Breaches Survey (Department for Digital, Media, Culture & Sport 2019) reports that 60+% of medium and large size firms in the UK "*have identified [cyber] breaches or attacks*". In the year to June 2019, the Office for National Statistics (2019) cites 977,000 incidences of computer misuse for England and Wales alone, a figure including both personal and business-related hacking attempts. With the Data Protection Act (2018) now in force in the UK along with the equivalent 'General Data Protection Regulation' (GDPR) EU wide, firms must disclose any breaches involving personal data within 72 hours and face hefty fines of up to €20m or 4% of turnover (whichever is the greater) for failure to comply.

In light of the above, as well as some recent high profile data breach disclosures such as that of British Airways (Bloomberg 2018), it would be reasonable to expect cyber security to be a major concern at board level for not only UK firms, but across Europe, and this research aims to investigate the impact of data breach announcements on the market value of publicly listed companies with a view to influencing investment in cyber security. Existing literature in this area was found to be somewhat sparse recently and exhibited a strong US bias, hence this paper will focus on European markets and compare/contrast with the literature.

B. Research Aims and Objectives

The primary aim of this research is to encourage firms (especially European listed) to invest in improving their cyber security posture through an understanding of the impact of data breach disclosures on market price. As well as adding to and updating the existing knowledge base of the economic impact of data breaches, another objective of this research would be to gain an understanding of differences between European markets and, in particular, the (more well researched) US markets in terms of the impact of data breach announcements.

The following research questions were proposed in order to achieve the research aims and objectives:

RQ1 What is the impact on company market value of a publicly announced data breach?

RQ2 Through detailed analyses of the share price data can any patterns/correlations be found?

RQ3 How can these findings be incorporated into companies' cyber security investment strategies?

RQ4 How does the data compare with existing literature?

C. Research Benefits

By gaining an up to date understanding of any potential negative impact of data breach related announcements on market value, this will highlight the importance of information security to business management as well as the need to invest in cyber security to avoid such incidents. Such insight would also assist practitioners of information security with business case justifications. This research would be of benefit to business management, practitioners of cyber security, investors and shareholders as well as researchers in cyber security or related fields.

II. RELATED WORK

The impact of publicly announced data breaches on market value (RQ1) is a topic which has been researched for some years. For example, Cavusoglu, Mishra, and Raghunathan (2004) reported that those firms suffering a serious data breach lost, on average, 2.1% of their market value within two days of the announcement, whereas Goel and Shawky (2009) cite a figure of around 1%. A recent literature review carried out by Spanos and Angelis (2018) noted that research in this area, despite its longevity, was "*quite limited"* although the majority (76%) of studies did show an impact of security

events on company market value which was statistically significant. Indeed, even more recently, Lin et al. (2020) cited a loss of 1.44% on average over 5 days. Tweneboah-Kodua, Atsu and Buchanan (2018: 646), who analysed breach events for 96 S&P500[1] listed firms between 2013 and 2017, however did not find significant impact over shorter event windows and warn that "*studying the cumulative effects of cyberattacks on prices of listed firms using event study methodology without grouping the firms into various sectors may not be informative*". Financial services sector firms, for example, showed larger abnormal returns over a 3-day event window than those in the technology sector, starting to provide input to RQ2.

Consistent with Tweneboah-Kodua et al. (2018), Richardson, Smith and Watson (2019) also report a lesser effect on market price, citing an average of less than 0.3% based on an analysis of 827 breach disclosures for 417 companies. Again, this was a US based study, the breach event data sourced from Privacy Rights Clearinghouse[2] (PRC). Richardson et al. (2019) chose propensity matched firms as a reference market rather than the more usual S&P500 composite index which could explain why their findings are so different from Cavusoglu et al. (2004). Indeed, Kannan, Rees and Sridhar (2007) in their study found no significant impact either, also using control firms as a reference. An alternative explanation is provided by Yayla and Hu (2011) who note that the market appears to have become less sensitive to breach events in recent years – another factor to be mindful of in any analyses.

Commenting on their findings, Richardson et al. (2019: 249) argue that "*companies are unlikely to change their investment patterns unless the cost of breaches increases dramatically or regulatory bodies enforce change*" – a contribution towards RQ3. It is acknowledged, however, by Richardson et al. (2019) that exceptional events do occur with cases of massive data exposure having potentially catastrophic impact, suggesting a need to categorise data breaches according to their severity (RQ2), such as number of records exposed or level of data sensitivity. Campbell et al. (2003) observed that breaches involving unauthorised access to confidential data were more likely to result in significant negative market reaction.

The above quotation from Richardson et al. (2019) also poses another question – what of the recent change of legislation (GDPR) in UK/EU, has there been any impact? As the introduction of GDPR is so recent (2018), literature in this area is rare, however Goel and Shawky (2014) carried out a similar US based study and observed that negative effects of security breaches were reduced significantly after the enactment of security breach notification laws. In a recent study of the economic impact of GDPR infringement fine disclosures, Ford et al. (2021) observed negative returns of around 1% up to 3 days after the announcement with this loss of market valuation being far greater than the monetary value of the fine itself in almost all cases. Seemingly minor fines could result in huge losses even for firms having large market capitalisations.

In summary, although there have been differences in results from studies related to the impact of data breach disclosures on market value, there are certainly some common themes such as: event study techniques (described below) are the favoured method for quantitative analyses and the research has a strong US bias, presumably because of readily accessible breach datasets for that market as well as a kind of 'one size fits all' market reference index in the S&P500, with a few notable exceptions such as Bose & Leung (2014). Thus, this research aims to go some way to address the deficit of European centric studies in this area although it should be recognised that literature searches were limited to English language only thereby possibly excluding some studies of interest.

III. Methodology

A. Overview

The high-level approach to this research will be to gather a dataset of data breach announcements for European publicly listed companies, then analyse the impact of these announcements on share price using an event study based approach.

B. Event Studies

Event studies have been widely used to assess the impact of specific events on the share price of firms and thereby their market value and are described in detail in, for example, MacKinlay (1997). A key assumption of this methodology is the ability of the market to reflect all available information as per the efficient market hypothesis (e.g. Fama 1970). By observing share price movements in reaction to information regarding a specific event, such as a data breach announcement over a short time period (the event window), it is possible to deduce how the market reacted to that specific event, given there are no other confounding events during that time-period.

A common approach used in similar (data breach type) event studies is the market model (e.g. Cavusoglu et al. 2004; Andoh-Baidoo, Amoako-Gyampah & Osei-Bryson 2010; Hinz et al. 2015; Schatz & Bashroush 2016; Castillo & Falzon 2018; Tweneboah-Kodua et al. 2018; Jeong, Lee & Lim 2019)

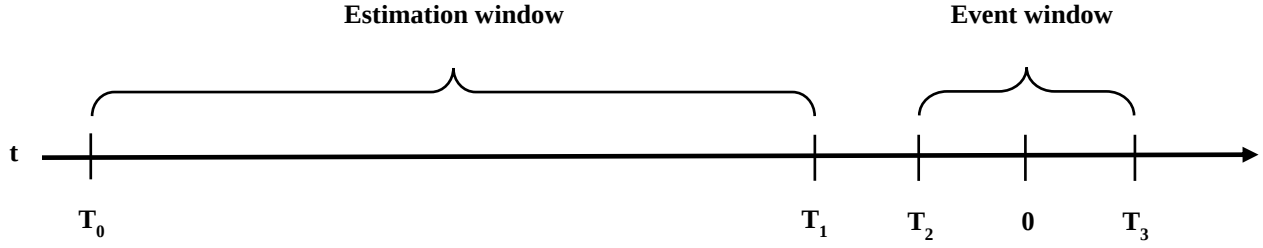

Figure 1: Event study timeline

[1] Standard & Poor's index of 500 US stocks representative of US markets in general

[2] https://privacyrights.org/

which uses an estimation window prior to the (shorter) event window (see Figure 1) to predict movement of the firm's stock based on a regression analysis. Returns are assumed to 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 (β_i) offset by its abnormal return (α_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 for *N* events as shown in equation (**4**).

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

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

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

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

The market model has been shown to stand up well against three and four factor models in similar studies. For example, Deane et al. (2019: 117) reported that the Fama–French–Carhart (four factor) model "*did not substantially differ from the market model*", an observation echoed by Richardson et al. (2019), Rosati et al. (2019) and Lin et al. (2020).

C. Data Collection

The scope for data collection was limited to breach announcements for companies (or their ultimate parents) publicly listed on a European exchange. Ownership of subsidiaries was confirmed through Dun & Bradstreet[3]. To maximise the initial data set, a broader geographic concept of Europe was used including both continental and trans-continental countries, 52 ISO-3166 country codes in total.

The manual data gathering exercise for European data breaches is described by the following steps (other breaches of relevance identified serendipitously were added, of course):

1. Review monthly cyber security blogs[4] for data breach announcements from 01/01/2017 stopping at 31/12/2019 (to avoid possible market effects of COVID-19 which could be considered a long-term confounding event in itself). The resulting dataset would be centred roughly around the introduction of GDPR in May 2018 to help with before/after comparisons.
2. Identify breaches of interest, namely those specific to European listed companies (or subsidiaries of European listed companies). Breach announcements regarding technology vulnerabilities which applied to multiple companies were disregarded. Privately owned companies were filtered out (e.g. Monzo, Yves-Rocher). Non-European examples filtered out included Everis Spain (Japan) and Three UK (Hong Kong). Also filtered out were cases where the 'breach' was only an allegation and the parent company immediately denied any breach had occurred e.g. Choice Hotels, British Airways.
3. Perform internet searches for the earliest dated public announcement (thereby removing uncertainty around the event date). In each case the announcement was validated against multiple later disclosures.
4. Where possible, additional data fields were gathered such as the nature of the breach, number of breached records and whether the incident involved personal data.

After completing the above steps, the resulting dataset comprised 33 records. To supplement these, a useful potential data source relevant for Europe mentioned in the literature was the Breach Level Index (BLI) as provided by Gemalto (Thales Group 2017), however since its acquisition by Thales, this data source seems to be no longer publicly available. Instead, the VERIS Community Database (VCDB)[5] was also reviewed as a possible data source, but data here was found to be sparse (only 8,857 records in total worldwide to date) having very little overlap with the hand-gathered dataset (actually only one, the UniCredit SpA incident). The original dataset was augmented by 12 breach disclosures as a result of the VCDB search bringing the total to 49 records. Such a sample size is nowhere near that used by e.g. Richardson et al. (2018) of 827 records but, nevertheless, closer to that of Tweneboah-Kodua et al. (2018) at 96. The difficulty of obtaining a breach database of similar size to these US based studies does, again, underpin favouritism towards this market by researchers due to accessibility of data and highlight the need for a European equivalent as there is no reason to believe European companies are not just as susceptible to data breaches as their US counterparts!

Share price and market index data were sourced from Yahoo!Finance (2019) along with firm demographics such as industry sector. For each ultimate parent company, the most appropriate reference index was selected, ideally one of which the candidate firm was a component but adjusted to closest match when data could not be extracted from Yahoo!Finance. This selection of the reference market is important (Kannan et al. 2007; Richardson et al. 2019). Some firms had multiple listings in which case the primary listing was favoured along with the associated index. Share price data were not available for all of the 49 records and a further four had to be removed namely Npower, Quickbit and Debenhams (no longer listed) as well as CD Projekt Red (no data currently available pre-2021). This left 45 events going forwards for analysis.

D. Data Analysis

To facilitate the analyses, R (R Core Team 2018)[6] scripts were developed to extract share price and index data directly from Yahoo!Finance for each of the 45 events and then event studies run using an R package (Schimmer, Levchenko & Müller 2014)[7] using the market model as described above. Non-trading event days were defaulted to the next available trading day. An estimation window of 120 days was chosen

[3] https://www.dnb.com

[4] Such as https://itgovernance.eu/blog and https://databreaches.net

[5] http://veriscommunity.net/vcdb.html

[6] R version 4.0.3 (2020-10-10)

[7] EventStudy package version 0.36.900 (API version 0.374-alpha)

consistent with e.g. Goel and Shawky (2009), Andoh-Baidoo et al. (2010), Schatz and Bashroush (2016), Richardson et al. (2019). In all cases the estimation window ended one trading day before the event window. Tweneboah-Kodua et al. (2018: 641) 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). Previous studies have shown market reaction before the event date due to information leakage. For example, using event study techniques, Lin et al. (2020) show significant evidence of opportunistic pre-official announcement insider trading related to data breaches. For this study, a range of event windows were initially chosen starting from up to two days before the event and varying in length from two to fifty[8] trading days in order to give visibility of these effects and others such as sector specific effects reported by e.g. Tweneboah-Kodua et al. (2018).

E. Hypothesis Development

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

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

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

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

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

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

This approach to significance testing is consistent with e.g. Castillo and Falzon (2018), Deane et al. (2019) and Jeong et al. (2019). Indeed, Deane at al. (2019: 115) state 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*".

[8] The limit of this software for CAR event windows was 50 days. For longer windows the buy-and-hold abnormal return (BHAR) approach is recommended.

RESULTS AND DISCUSSION

To identify any significant CAR (RQ1) an initial visualisation similar to Figure 3 showed that Travelex was a major outlier (having a CAR of -75% over a 3-day window) and would fall into the category which Richardson et al. (2019: 248) describe as *"those rare situations involving massive data exposures"*. The company has since gone into administration citing both the cyber-attack and COVID-19 effects as contributing factors (The Guardian 2020). Since this event occurred on 31/12/2019 it was at the limit of the data selection range and the event window would certainly extend into potential 'COVID-19 territory'. Therefore, Travelex was excluded from further analyses leaving 44 breach events remaining. These residual events were re-visualised as shown in Figure 3. No obvious evidence of information leakage prior to the announcement date (e.g. Lin et al. 2020) was observed with, in fact, slightly positive CAAR being observed for event windows (-2, 2), (-1, 1) and (-1, 0). Studies where there was uncertainty around the announcement date favoured event windows such as these to ensure abnormal returns were not missed (e.g. Schatz & Bashroush 2016) but here all dates were validated. Nevertheless, the expectation based on previous studies would be to see market reaction kicking in 1-2 days after the event, growing to a maximum and disappearing over longer event windows. What can be seen here is that the market reaction appears to be much slower overall with no visible negative trend until the (0, 5) window at the earliest, disappearing the following day and subsequently reappearing a month after the event (0, 20). These longer windows operating at the outer limits of event study methodology also seem to be skewed by outliers such as NatWest enjoying, surprisingly, a positive run following their breach announcement and Fox-IT along with The AA falling over 20%. That Fox-IT, a cyber security specialist company itself, suffered such a negative market reaction would certainly come as no surprise, albeit seemingly somewhat late. Clearly there is a need to look more deeply here into the nature of the businesses affected (beginning to answer RQ2) as recommended by Tweneboah-Kodua et al. (2018) and Bendovschi, Al-Nemrat and Ionescu (2016).

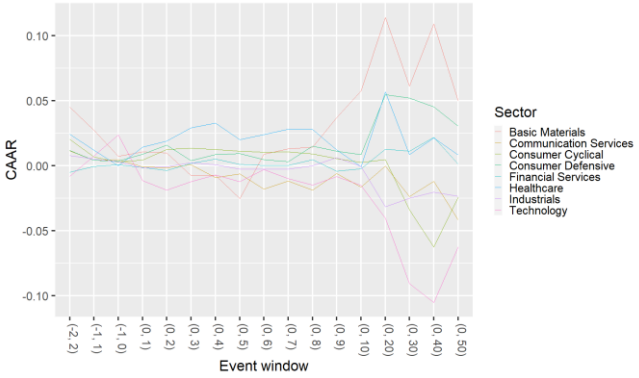

Figure 2: CAAR by industry sector

For this purpose, a graph of CAAR by sector for each event window is shown in Figure 2. It appears that the fastest negative reaction to a breach is, indeed, shown by the technology sector peaking two days after the disclosure in the short term. Financial and communication services companies

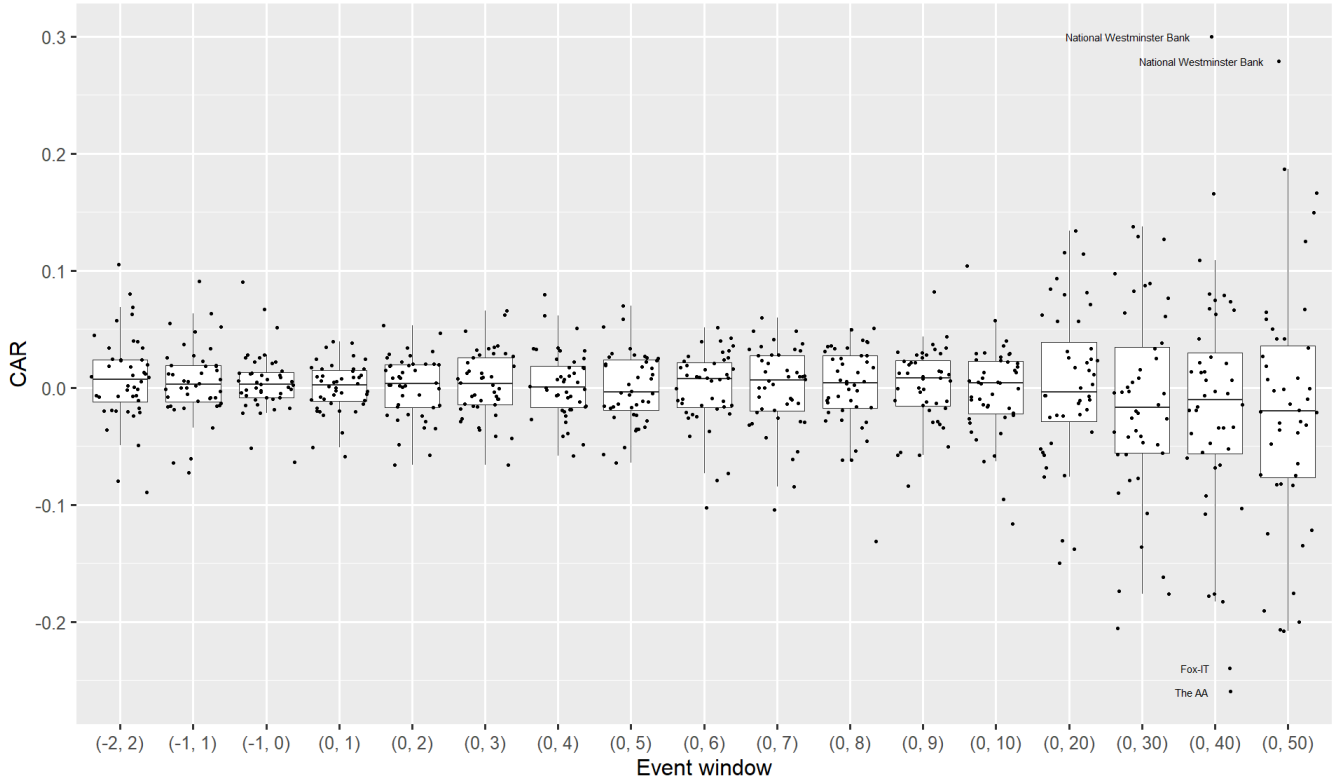

Figure 3: Boxplots of CAR values per event window

show little reaction at all over this time period which is somewhat unexpected based on previous studies. The basic materials sector shows the largest short term negative impact after five days although it should be noted that there was only one company (Norsk Hydro) assigned to this sector, so it made sense to choose the (0, 2) window for a closer look at sector performance. The results are shown in Table 1. Although 4 sectors show negative CAAR for this event window, the average impact is still slightly positive (0.001) over all 44 events and the negative CAARs are not statistically significant thus we cannot reject the null hypothesis for these. However, the CAAR is significant at the 5% level for the consumer defensive sector but in a positive way with the share prices rising over 1% in response to the breach disclosure. Companies in this sector, however, could reasonably be expected to outperform under adversity due to their defensive nature.

Not having found evidence of negative impact so far, the observation of Richardson et al. (2019) regarding massive breach volumes leading to more serious effects warrants investigation. Where it was possible to gather an indication of the number of records breached, this information was added to the dataset (25 examples). It can be seen that the financial services sector was responsible for over 99% of all the records breached, in all cases involving sensitive (personal) data and the majority (55%) being GDPR relevant, thus it seems somewhat surprising the market reaction is not more severe.

Table 1: Analysis of event window (0, 2) by sector

Industry Sector	N	CAAR	S_{CAAR}	t_{CAAR}	Negative CAR %	Total Records Breached	Personal %	GDPR %
Technology	4	-0.0188	0.0390	-0.9656	50	-	75	75
Financial Services	11	-0.0036	0.0250	-0.4730	55	1,360,584,255	100	55
Communication Services	8	-0.0015	0.0193	-0.2124	50	3,117,453	88	75
Industrials	8	-0.0007	0.0345	-0.0574	38	404,700	50	75
Basic Materials	1	0.0098			0	-	0	100
Consumer Cyclical	8	0.0124	0.0250	1.4021	25	358,000	88	75
Consumer Defensive	3	0.0158	0.0034	7.9690**	0	17,295	33	67
Healthcare	1	0.0190			0	-	0	100
	44	**0.0010**			**39**	**1,364,481,703**	**75**	**70**

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

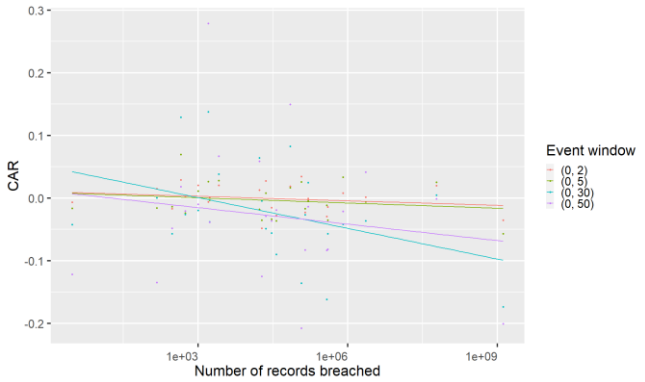

Figure 4: CAR versus records breached

Figure 4 gives an idea of a correlation between the number of records breached (logarithmic scale) and CAR for a selection of the more interesting event windows. There appears to be a weak trend that CARs become more negative the more records there are breached which becomes stronger with the longer windows. As event studies are better suited to the days immediately surrounding it was decided to focus on other, more major factors. Campbell et al. (2003) noted that breaches involving sensitive personal data led to more negative CARs. For this reason, the sector analysis in Table 1 was rerun restricting the dataset to only those events involving sensitive (personal) data and the results are shown in Table 2. This had the effect of altering the mean CAAR from a slightly positive value to a slightly negative value (0.001 to -0.001). Despite the reduction in events to 33, the financial services sector was unaffected meaning all 11 events involved sensitive data. The technology sector became 37% more negative yet the results are still not statistically significant for any sector. Thus, the null hypothesis of zero abnormal returns still stands.

Table 2: Analysis of event window (0, 2) by sector (personal data)

Industry Sector	N	CAAR	S_{CAAR}	t_{CAAR}	Negative CAR %
Technology	3	-0.0259	0.0446	-1.0040	67
Communication Services	7	-0.0061	0.0152	-1.0623	57
Financial Services	11	-0.0036	0.0250	-0.4730	55
Industrials	4	0.0063	0.0266	0.4725	25
Consumer Defensive	1	0.0130			0
Consumer Cyclical	7	0.0138	0.0266	1.3720	29
	33	**-0.0008**			**45**

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

Goel and Shawky (2014) observe that the introduction of data breach notification laws led to a reduction in negative market reaction. For this purpose, Table 3 shows an analysis of abnormal returns for four particularly negative event windows, both before and after the enactment of the GDPR, for the above set of 33 events specifically involving personal data. In three of the four cases, pre-GDPR negative CAAR was turned positive after enactment and, even in the fourth case, the negative CAAR was reduced over 90%. Unfortunately, the results were only statistically significant (at the 10% level) for the longer event windows pre-GDPR and these longer-term event study observations are known to be less reliable.

Table 3: Market effect of GDPR enactment

Event Window	GDPR	N	CAAR	S_{CAAR}	t_{CAAR}	Negative CAR %
(0, 2)	PRE	12	-0.0079	0.0267	-1.0260	50
(0, 2)	POST	21	0.0033	0.0257	0.5953	43
(0, 5)	PRE	12	-0.0114	0.0281	-1.4023	75
(0, 5)	POST	21	0.0039	0.0303	0.5946	48
(0, 30)	PRE	12	-0.0564	0.0916	-2.1330*	83
(0, 30)	POST	21	-0.0047	0.0791	-0.2702	57
(0, 50)	PRE	12	-0.0592	0.1101	-1.8645*	83
(0, 50)	POST	21	0.0022	0.1135	0.0881	62

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

Finally, an analysis by market reference was carried out (Table 5) to give, effectively, a geographic breakdown and see which markets were more sensitive to data breach announcements. Of the shorter event windows, (0, 1) proved to be of particular interest as this was the first real evidence of a statistically significant abnormal return (at the 5% level), specifically related to the Spanish market (IBEX35). Although there were only four breach events relevant to this market, they spanned three different industry sectors, three out of four were GDPR relevant, and half and half sensitive versus non-sensitive data therefore, it seems, the market itself was the common factor here. One of these breaches was, however, by far the largest (TSB/Sabadell) so volume could have played a part. The most negative impact for this 2-day window was that of the AEX25 (Netherlands) at around -3.8%, but there was only one example here (ING Bank). It is interesting to note that the FTSE350[9] index would effectively cover 17 (39%) of the events so there was a strong UK bias here. As an additional check on the importance of the reference index (Kannan et al. 2007; Richardson et al. 2019), the sector analysis (Table 1) was rerun using the SPEUR350[10] as a reference across all events. The resulting abnormal returns are shown in Table 4.

Table 4: Analysis of event window (0, 2) by sector (SPEUR350)

Industry Sector	N	CAAR	S_{CAAR}	t_{CAAR}	Negative CAR %
Technology	4	-0.0213	0.0356	-1.1955	50
Financial Services	11	-0.0051	0.0241	-0.7056	45
Communication Services	8	-0.0003	0.0199	-0.0445	38
Industrials	8	0.0000	0.0369	-0.0010	38
Consumer Cyclical	8	0.0107	0.0243	1.2415	38
Consumer Defensive	3	0.0165	0.0080	3.5875*	0
Basic Materials	1	0.0179			0
Healthcare	1	0.0248			0
	44	**0.0008**			**36**

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

[9] The FTSE100 and FTSE250 combined.

[10] Standard & Poor's index of 350 stocks representative of European markets in general

Table 5: Analysis by market index for event window (0, 1)

Reference Market	Country	N	CAAR	S_{CAAR}	t_{CAAR}	Negative CAR %	Total Records Breached	Personal %	GDPR %
AEX25	NL	1	-0.0383			100	19,055	100	100
OMXH25	FI	1	-0.0237			100	-	100	100
FTSEMIB	IT	1	-0.0207			100	400,000	100	0
ATXPRIME	AT	1	-0.0200			100	-	0	100
IBEX35	ES	4	-0.0098	0.0038	-5.1543**	100	1,300,000,000	50	75
FTSE250	GB	7	-0.0067	0.0366	-0.4858	43	240,000	86	57
CAC40	FR	5	0.0005	0.0163	0.0631	60	181,300	100	80
FTSE100	GB	10	0.0053	0.0136	1.2364	30	398,753	80	70
ISEQ20	IE	2	0.0056	0.0063	1.2472	0	845	50	50
DAX30	DE	7	0.0069	0.0205	0.8980	57	2,440,750	71	86
MOEX50	RU	1	0.0090			0	60,000,000	100	100
OSEAX†	NO	1	0.0107			0	-	0	100
SMI20	CH	1	0.0161			0	800,000	100	0
OMXCBGI‡	DK	2	0.0219	0.0184	1.6846	0	1,000	50	50
		44	**0.0001**			**48**	**1,364,481,703**	**75**	**70**

,**, Indicate statistical significance at the 10%, 5% and 1% levels respectively.**
† OBX25 not available
‡ OMXC25 not available

The overall mean CAAR only differs by 0.0002 and the results look very similar, with again only the consumer defensive sector showing statistical significance but this time only at the 10% level. Using market specific indices produced higher t_{CAR} values on average so this was the preferred method (cf. Bose & Leung 2014).

CONCLUSION

Overall we have seen no clear impact on share price of data breach announcements (RQ1) in European companies across all sectors and markets other than Spain. Based on this evidence it is difficult to support business cases for investment in cyber security measures (RQ3), although there could be other approaches as Deane et al. (2019) report a significant uplift in share price for organisations following an announcement related to security certification. Thus, justification for investment would have to depend on other factors such as risk appetite (no company wants to be the next Travelex), industry sector, nature of the data compromised and relevant legislation. These findings are consistent with Richardson et al. (2019) who refer to their observations on the (lack of) economic impact of data breach announcements as "*much ado about nothing*" yet other, mostly earlier, US based research in this area did find significant evidence of negative market reaction supporting the finding of Yayla and Hu (2011) that markets were becoming less sensitive to data breach disclosure over time. That said, the Spanish market (RQ2) showed statistically significant and rapid sensitivity to data breach announcements, continuing after the enactment of GDPR. Other European markets showed a slight reduction in negative CAR post-GDPR as predicted by Goel and Shawky (2014) but, again, not statistically significant. At the time of writing the Spanish data protection authority (AEPD) has issued more GDPR infringement fines (236 examples) than any other (CMS Legal 2021) so perhaps this is a contributing factor to the higher market sensitivity towards data breaches in Spain.

Some differences with US markets were identified, for example, the slower response of the European financial services sector (RQ4). The specific case of Travelex also fits with the observations of Richardson et al. (2019) that in the case of particularly severe breaches, the situation may become irrecoverable, although COVID-19 was cited as a contributing factor in its demise. Following on from this some evidence of a (weak) correlation between negative CAR and number of records breached was identified, but not really in the short term. Nevertheless, this should be borne in mind for any risk assessment along with the nature of the data itself.

One shortcoming identified as part of this research was the lack of a publicly available breach database like, for example, PRC which features heavily in similar US based studies. Although the VCDB project seems well-intentioned as a global research resource, what is really needed is a much more comprehensive and richer dataset in order to study European and other markets to a depth equivalent to that of US research in this area. Although this study has begun to look at the economic impact of GDPR this is another potential area for future research once the market stabilises and more data becomes available. It must be recognised that these disclosure events are early in the cyber security incident lifecycle and, although appearing no more than a nuisance to the markets generally, there may well be more surprises to follow depending on how effectively they are managed.

ACKNOWLEDGEMENTS

The authors wish to thank the anonymous reviewers for their valuable and constructive feedback.

REFERENCES

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

Bendovschi, A., Al-Nemrat, A., Ionescu, B. (2016), *Statistical Investigation into the Relationship between Cyber-Attacks and the Type of Business Sectors*, International Journal of Business, Humanities and Technology, (**6**)1, 49-61

Bose, I., Leung, A.C.M. (2014), *Do phishing alerts impact global corporations? A firm value analysis*, Decision Support Systems, **64**, 67-78.
Bloomberg (2018), *IAG Share Price Hit After British Airways Data Hack*, https://www.bloomberg.com/news/articles/2018-09-06/british-airways-says-hackers-stole-customers-credit-card-data. Accessed on: 11/06/2021
Campbell, K., Gordon, L.A., Loeb, M.P., Zhou, L. (2003), *The economic cost of publicly announced information security breaches: empirical evidence from the stock market*, Journal of Computer security, **11**(3), 431-448.
Castillo, D., Falzon, J. (2018), *An analysis of the impact of Wannacry cyberattack on cybersecurity stock returns*, Review of Economics and Finance, **13**(3), 93-100
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
CMS Legal (2021), GDPR Enforcement Tracker, https://www.enforcementtracker.com/?insights. Accessed on: 11/06/21
Data Protection Act (2018), http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted. Accessed on: 11/06/2021
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
Department for Digital, Media, Culture & Sport (2019), *Cyber Security Breach survey 2019*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/791943/CSBS_2019_Infographics_-_Micro_and_Small_Businesses.pdf. Accessed on: 11/06/2021
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. (2021), *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
The Guardian (2020), *Travelex falls into administration, with loss of 1,300 jobs*, https://www.theguardian.com/business/2020/aug/06/travelex-falls-into-administration-shedding-1300-jobs. Accessed on: 10/06/21
Goel, S., Shawky, H.A. (2009), *Estimating the market impact of security breach announcements on firm values*, Information & Management, **46**(7), 404-410
Goel S., Shawky H.A. (2014) *The Impact of Federal and State Notification Laws on Security Breach Announcements*, Communications of the Association for Information Systems, **34**, 37-50
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
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
MacKinlay, A. C. (1997), *Event Studies in Economics and Finance*, Journal of Economic Literature **35**(1) (March)
Office for National Statistics (2019), *Crime Survey England & Wales 2019*, https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingjune2019/pdf. Accessed on: 11/06/21
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
Rosati, P., Deeney, P., Cummins, M., Van der Werff, L., Lynn, T. (2019), *Social media and stock price reaction to data breach announcements: Evidence from US listed companies*, Research in International Business and Finance, **47**, 458-469
R Core Team (2018), *R: A language and environment for statistical computing*. R Foundation for Statistical Computing, Vienna, Austria, https://www.R-project.org/. Accessed on: 11/06/21
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., Müller, S. (2014), *EventStudyTools (Research Apps), St.Gallen*, http://www.eventstudytools.com. Accessed on: 11/06/21
Spanos, G., Angelis, L. *The impact of information security events to the stock market: A systematic literature review* (2016) Computers and Security, **58**, 216-229
Thales Group (2017), *First half 2017 Breach Level Index report*, https://www.thalesgroup.com/en/markets/digital-identity-and-security/press-release/first-half-2017-breach-level-index-report-identity-theft-and-poor-internal-security-practices-take-a-toll. Accessed on: 10/06/21
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
Yahoo!Finance (2019), *Historical Data*, https://finance.yahoo.com/quote. Accessed on: 11/06/21
Yayla, A. A., Hu, Q. (2011), *The Impact of Information Security Events on the Stock Value of Firms: The Effect of Contingency Factors*, Journal of Information Technology, **26**(1), 60–77