The Impact of GDPR Infringement Fines on the Market Value of Firms

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

DOI: 10.34190/EWS.21.088

Abstract: Previous studies have shown (varying degrees of) evidence of a negative impact of data breach announcements on the share price of publicly listed companies. Following on from this research, further studies have been carried out in assessing the economic impact of the introduction of legislation in this area to encourage firms to invest in cyber security and protect the privacy of data subjects. Existing research has been predominantly US centric. This paper looks at the impact of the General Data Protection Regulation (GDPR) infringement fine announcements on the market value of mostly European publicly listed companies with a view to reinforcing the importance of data privacy compliance, thereby informing cyber security investment strategies for organisations. Using event study techniques, a dataset of 25 GDPR fine announcement events was analysed, and statistically significant cumulative abnormal returns (CAR) of around -1% on average up to three days after the event were identified. In almost all cases, this negative economic impact on market value far outweighed the monetary value of the fine itself, and relatively minor fines could result in major market valuation losses for companies, even those having large market capitalisations. A further dataset of four announcements where sizeable GDPR fines were subsequently appealed was also analysed and although positive returns for successful appeals were observed (and the reverse), they could not be shown to be statistically significant - perhaps due, at least in part, to COVID-19 related market volatility at that time. 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 (pointers to future research are given). Data protection authorities may also find this work of interest.

Keywords: cyber security, data privacy breaches, market value, economic impact, GDPR, event study

1. Introduction

The European Union Agency for Cybersecurity (ENISA, 2020) reported a *"54% increase in the total number of [data] breaches by midyear 2019 compared with 2018"*. Regarding the introduction of the General Data Protection Regulation (GDPR) in May 2018, ENISA also remark that *"55% of the responders to a Eurobarometer survey responded that they are concern[sic] about their data being accessed by criminals and fraudsters"*. Clearly there is major concern out there in the field of data privacy. The primary objective of the GDPR is to protect "*fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data*" (Data Protection Act 2018). The requirement, therein, to notify data breaches to the relevant supervisory authority within 72 hours of becoming aware (where feasible), could reasonably be expected to increase visibility of non-compliance. For example, in the UK, before the introduction of the GDPR as the Data Protection Act (DPA), 2018, the preceding DPA (1998), according to the Information Commissioner's Office (ICO)[1], stated "*although there is no legal obligation on data controllers to report breaches of security which result in loss, release or corruption of personal data, the Information Commissioner believes serious breaches should be brought to the attention of his Office.*" Prior to 2010, the ICO were limited to serving enforcement notices for contraventions of the DPA (1998), however in April 2010 the ICO was granted the power to issue fines of up to £500,000 on its own authority. For example, Sony Computer Entertainment Europe were fined £250,000 in January 2013 for a "*serious breach*" when their PlayStation Network was hacked (BBC 2013) and in 2016, TalkTalk were fined £400,000 for leaking personal data of almost 157,000 customers due to poor website security (BBC 2016). Serious infringements under the GDPR, those violating the fundamental principles of the right to privacy and the right to be forgotten, could result in a fine of up to €20 million or 4% of the firm's worldwide annual revenue from the preceding financial year (whichever amount is higher), a clear deterrent against carelessness concerning data privacy and security. Indeed, total fines issued by data protection authorities since the introduction of the GDPR currently stand at over €275m (CMS Legal 2021).

This research is concerned with the impact the announcement of such GDPR fines has on the market value of publicly listed companies. Spanos and Angelis (2016) report that data breach announcements are associated with a negative impact on market value. Could it be that, since the introduction of the GDPR, a firm's share price

[1] The supervisory (data protection) authority of the UK (https://ico.org.uk)

may suffer a 'double whammy' of both initial breach notification and subsequent punitive action? This paper aims to assess the economic impact of the introduction of the GDPR on publicly listed companies through the application of fiscal penalties levied by its supervisory authorities on those firms which have suffered a data privacy breach. By gaining a greater understanding in this area it is hoped to encourage firms to invest more in cyber security measures to prevent such occurrences. To achieve this objective, the following research questions were considered:

- Is there any impact on company market value of a publicly announced GDPR fine?
- Do data analyses reveal any obvious patterns/correlations?
- What is the impact of any fine successfully appealed and subsequently overturned or reduced?
- How can the results inform cyber security investment strategies?
- Can any conclusions be drawn about the introduction of the GDPR itself?

This research will highlight the importance of data privacy and protection to business management and thus the need to invest in and improve their organisation's cyber security posture[2] thereby reducing the risk of data privacy breaches. 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. It could also be of value to data protection authorities to increase their understanding of the impact and enforcement of legislation on the economy. Another benefit of this study would be the European focus thereby beginning to offset the strong US bias of the existing literature in this area.

2. Related work

A systematic literature review concerning the impact of data breach events on the stock market carried out by Spanos and Angelis (2016) reports that, although research in this area was "*quite limited*", the majority of studies (76%) found a statistically significant negative impact. For example, Lin et al. (2020) report a loss of 1.44% on average over a 5-day window. Andoh-Baidoo, Amoako-Gyampah and Osei-Bryson (2010) report -3.18% abnormal returns over a 3-day period. Cavusoglu, Mishra and Raghunathan (2004) cite -2.1% on average within two days after the announcement. Goel and Shawky (2009) quote -1% in the days surrounding the event. These studies also note some correlations between these negative returns and, for example, industry sector. Tweneboah-Kodua, Atsu and Buchanan (2018), warn that "*studying the cumulative effects of cyberattacks on prices of listed firms without grouping them into the various sectors may be non-informative*". They noted that financial services firms reacted more rapidly and more significantly than those in the technology sector. It was also observed by Campbell et al. (2003) that those breaches involving unauthorised access to confidential data were more likely to result in significant negative market reaction, which one would reasonably expect to apply across the board for this study. Such observations would support the idea of governments introducing legislation to not only counter this negative economic impact but also to help protect data subjects who are effectively innocent victims of such breaches of confidentiality. Indeed, the right to privacy is a component of the European Convention on Human Rights (1950) and the EU has sought to protect this right through legislation ever since with, firstly, the introduction of the European Data Protection Directive (1995) then the Privacy and Electronic Communications Directive (2002) and, in response to ever-evolving technology and increases in data transfers, the GDPR in 2018 along with the (delayed) ePrivacy Regulation due to repeal the 2002 Directive (European Commission 2021).

This relatively recent introduction of the GDPR naturally limits the availability of research on its impact, so it is necessary to look elsewhere. The introduction of data breach notification laws in the US was found to reduce identity theft by over 6% on average (Romanosky, Telang & Acquisti 2011). Clearly if data subjects are rapidly made aware their personal data has been compromised, and which data, they should be better positioned to take preventative action. There are already, however, some criticisms of the effectiveness of the GPDR in this area as notification to data subjects is only required in certain *"high risk"* cases and where it would not place too onerous a burden on the reporting organisation (Nieuwesteeg & Faure 2018). Data breach notification laws have been widely adopted in the US, albeit not centrally – federal law in this area only covers certain specific sectors. Nevertheless, 47 jurisdictions have implemented their own notification legislation. In fact, the US could be considered an early adopter. In contrast the EU GDPR model is central and adopted by member states and

[2] Cyber security posture includes not only governance and technical solutions but also training and awareness.

includes the notification requirement within the data protection law itself unlike, for example, Australia (Daly 2018) where a separate law was introduced in early 2017. Goel and Shawky (2014) carried out a US based study examining the impact of data breach announcements on share price and found a significant reduction in negative returns after the enactment of both federal and state laws. Murciano-Goroff (2019) looked at Californian company investment in web server security following the introduction of state data breach notification law yet only noted a modest effect with server software being, at most, 2.8% newer. Indeed, Richardson, Smith and Watson (2019) argue that "*companies are unlikely to change their investment patterns unless the cost of breaches increases dramatically or regulatory bodies enforce change*" underpinning the need for an understanding of the impact and effectiveness of the GDPR on cyber security investment – an area which this research aims to inform as well as bringing an EU specific perspective to offset the strong US bias of previous studies.

3. Methodology

The high-level approach to this research was to download a list of publicly announced GDPR infringement fines from the Enforcement Tracker (CMS Legal 2021), filter this dataset for those cases involving publicly listed companies and analyse the impact of these announcements on share price using event study techniques.

3.1 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.

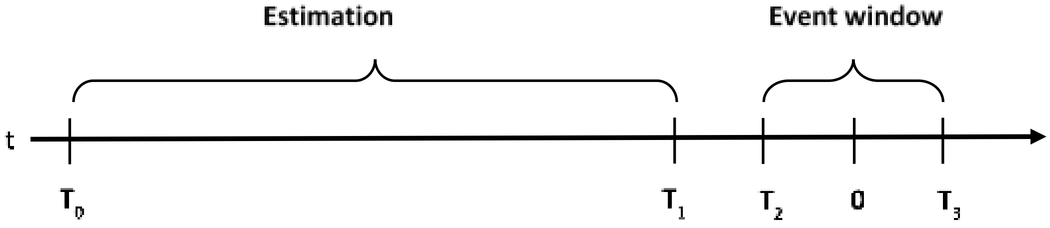

Figure 1: Event study timeline

A common approach used in similar (data breach type) 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) 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**).

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

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

$$CAR_i = \sum_{t=T_2}^{T_3} AR_{i,t} \tag{3}$$

$$CAAR = \frac{1}{N}\sum_{i=1}^{N} CAR_i \tag{4}$$

3.2 Data collection

The base dataset used to identify fine announcements was from the GDPR Enforcement Tracker. Although not professing to be an exhaustive list, when the data were downloaded in May 2020 this resulted in 277 records. Manually filtering these records for those involving publicly listed companies (or a subsidiary of a publicly listed company[3]) resulted in 71 rows. Some announcement dates were found to be missing and filled in from press reports and official data protection authority publications where applicable. It was necessary to exclude certain records due to a missing date such as Facebook (Germany) and Unicredit (Czech Republic/Slovakia). Events on the same day were consolidated into one e.g. Eni Gas e Luca, EDP Spain. Entries which had potentially overlapping event windows were also filtered e.g. Vodafone (2 events). Share price and market index data were extracted from Yahoo!Finance (2019) along with firm demographics such as annual revenue, market capitalisation and industry sector. Information was not available for all the events on Yahoo!Finance e.g. Louis Group (Cyprus), Xfera (now privately owned) and Avon Cosmetics (event was pre-public), thus these events had to be filtered out also, leaving 48 records. The most appropriate market index was chosen as a reference in each case (Kannan, Rees and Sridhar (2007) highlighted the importance of the market reference), ideally one which included the candidate company itself but adjusted, if needed, due to lack of availability of data in Yahoo!Finance. Some firms had multiple listings in which case the primary listing and associated index were used. The date range was limited, naturally, from the earliest fine since the introduction of the GDPR in 2018 (actually, January 2019) until the date of download but it was decided to cap the data at 31/12/2019 in order to avoid market uncertainties due to COVID-19, that being a long-term confounding event in itself. This date capping reduced the dataset from 48 to 25 events for analysis.

3.3 Data analysis

To facilitate the analyses, R (R Core Team 2018)[4] scripts were developed to pull share price and index data directly from Yahoo!Finance for each data record and then event studies run using an R package (Schimmer, Levchenko & Müller 2014)[5] 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 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) 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 2 up to 20 trading days to give visibility of these effects and others such as sector specific effects reported by e.g. Tweneboah-Kodua et al. (2018) who observed more rapid response from the financial services sector, for instance.

3.4 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**).

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

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

[3] Ultimate parent companies were identified from Dun & Bradstreet (https://www.dnb.com)

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

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

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**).

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

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

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*".

4. Results and discussion

Event studies were carried out as described above for 10 event windows of varying length across all 25 GDPR fine events. A visualisation of the overall results is shown in **Figure 2**. It appears at first glance that the most negative impact is seen around the 4-day event window (0, 3) with the market value gradually recovering over longer windows and beginning to see positive recovery 10 days after the event. After 20 days, for IAG (Vueling) and EDF (Madrileña Red de Gas) the abnormal returns had grown to over 10% either way yet the median CAR remained much closer to zero.

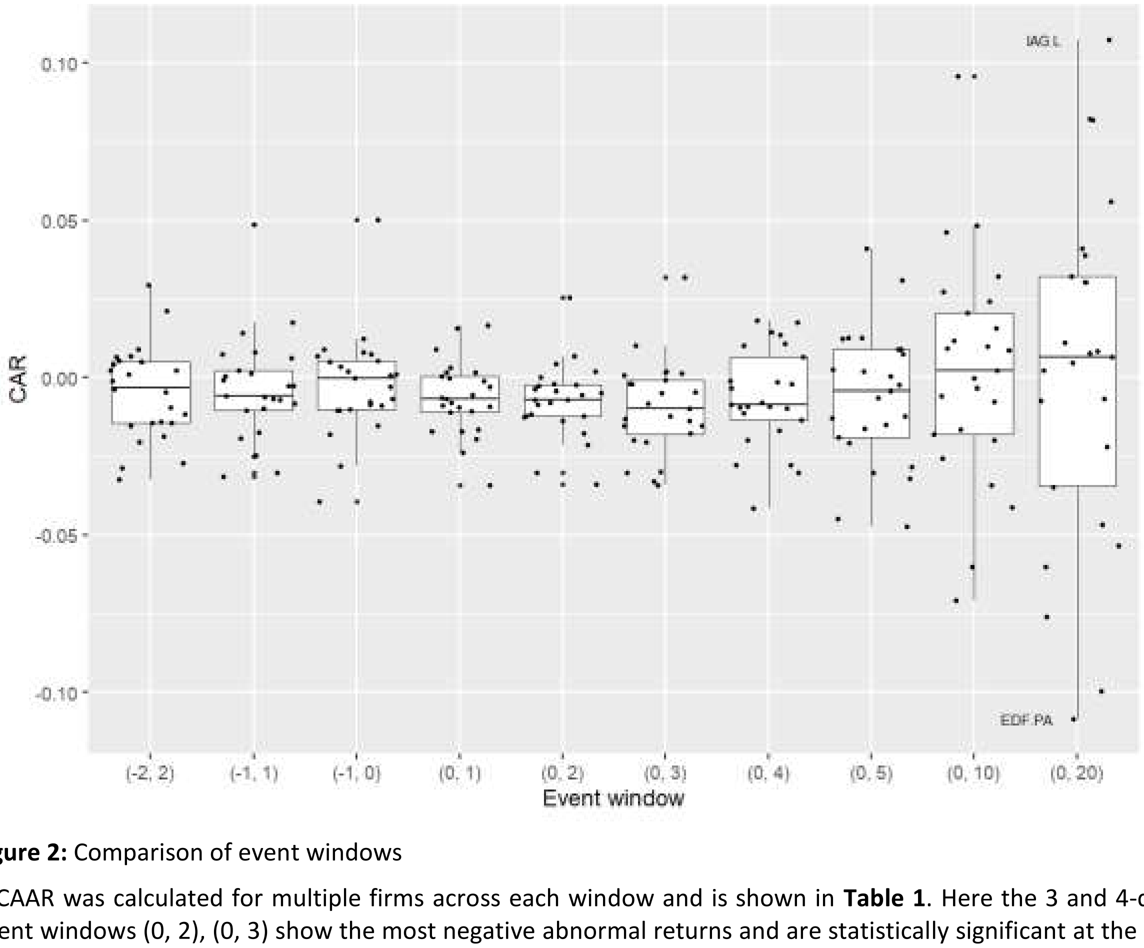

Figure 2: Comparison of event windows

A CAAR was calculated for multiple firms across each window and is shown in **Table 1**. Here the 3 and 4-day event windows (0, 2), (0, 3) show the most negative abnormal returns and are statistically significant at the 1% level. It is interesting to note that the null hypothesis cannot be rejected for the three earlier event windows involving pre-event days thereby indicating no information leakage prior to the fine announcements and consistent with the lack of uncertainty in the event dates for this exercise. As above, there is also lack of statistical significance for the longer windows indicative of a tendency of market recovery towards zero abnormal returns over time as reported by Dyckman et al. (1984). The event window (0, 3) showed the most negative (almost 1%) CAAR, consistent with the findings of Goel and Shawky (2009). Within this window, 19 of the 25 events (76%) had abnormal returns of less than zero, therefore this window was chosen as the basis for further analyses. Usage of this event window (0, 3) has been previously reported in studies of this type e.g. Hinz et al. (2015), Rosati et al. (2019).

Table 1: CAAR by event window

Event Window	N	CAAR	t_{CAAR}		% Negative CAR
(-2, 2)	25	-0.0049	-1.6188		56
(-1, 1)	25	-0.0041	-1.2112		64
(-1, 0)	25	-0.0022	-0.6746		52
(0, 1)	25	-0.0064	-2.7453	**	72
(0, 2)	25	-0.0072	-3.0748	***	80
(0, 3)	25	-0.0096	-3.2341	***	76
(0, 4)	25	-0.0064	-2.0190	*	72
(0, 5)	25	-0.0061	-1.4128		56
(0, 10)	25	0.0020	0.2795		48
(0, 20)	25	0.0011	0.0968		40
	250	**-0.0044**			**62**

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

An analysis by ultimate parent company of CAAR is shown in **Table 2**. It can be seen that four firms suffered more than one fine under GDPR, but no more than two during the date range of this study. The firm suffering the most negative abnormal return is listed first and the most positive last. The overall average fine levied was found to be almost €17m and it appears that the supervisory authorities have been relatively lenient so far with the average penalty sitting at around 0.15% of previous year's annual revenue (the greatest being just over 1%) and nowhere near the possible maximum of 4% for more serious GDPR infringements[6]. That said, the average loss in market capitalisation based on the CAAR was estimated to be of the order of nearly 29,000 times that at €1.2bn. Clearly this figure is heavily skewed by the €19bn loss Alphabet Inc. experienced following their €50m fine. It seems that a huge market value is little protection against abnormal returns with the smallest company in the sample, Österreichische Post, having a slightly positive return. Also noteworthy was the seemingly innocuous €2k fine for BNP Paribas precipitating a market value fall of nearly €1bn. It was also noted that there was only one case (Österreichische Post) out of all 25 where the ratio of change in market capitalisation to fine was less than one, so firms need to recognise that the overall financial impact of a GDPR penalty is likely to be much greater than the value of the actual fine itself.

Table 2: Analysis by ultimate parent company

Ultimate Parent Company	N	CAAR	Average Revenue † € 000,000	Average Fine € 000	Fine as % of Revenue	Market Capitalisation ‡ € 000,000	Δ Market Capitalisation € 000	Δ MC to Fine Ratio
United Internet	1	-0.0342	5,131	9550	0.1861	7,104	242,957	25
Endesa SA	1	-0.0300	19,555	60	0.0003	22,634	679,020	11,317
Iberdrola	2	-0.0253	35,076	42	0.0001	63,221	1,602,652	38,618
UniCredit	1	-0.0204	20,674	130	0.0006	18,639	380,236	2,925
Delivery Hero	1	-0.0198	665	195	0.0294	23,691	469,082	2,401
Alphabet Inc	1	-0.0153	120,380	50000	0.0415	1,245,280	19,052,788	381
BNP Paribas	1	-0.0152	52,030	2	0.0000	61,513	934,998	467,499
International Airlines	2	-0.0148	24,406	102315	0.4192	10,354	153,246	1

[6] Note that percentages were calculated based on ultimate parent revenues and not necessarily that of the infringing legal entity.

Ultimate Parent Company	N	CAAR	Average Revenue † € 000,000	Average Fine € 000	Fine as % of Revenue	Market Capitalisation ‡ € 000,000	Δ Market Capitalisation € 000	Δ MC to Fine Ratio
Vodafone	1	-0.0130	43,666	60	0.0001	40,960	532,482	8,875
Eni SpA	1	-0.0123	75,822	11500	0.0152	33,157	407,831	35
Deutsche Telekom	2	-0.0110	75,351	21	0.0000	70,219	768,898	36,614
Marriott	1	-0.0097	18,507	110390	0.5965	41,340	400,995	4
Enel SpA	1	-0.0049	74,221	6	0.0000	82,095	402,266	67,044
ING Group	1	-0.0046	18,304	80	0.0004	34,953	160,784	2,010
OTP Bank	1	-0.0019	2,955	511	0.0173	10,979	20,861	41
Direct Line Insurance	1	-0.0007	3,937	5	0.0001	4,954	3,468	694
Électricité de France	1	0.0014	68,976	12	0.0000	31,142	43,599	3,633
Engie SA	1	0.0016	60,596	60	0.0001	30,778	49,245	821
Österreichische Post	1	0.0019	1,958	18000	0.9191	2,320	4,408	0
Telefónica	2	0.0042	48,693	39	0.0001	20,019	84,080	2,156
Deutsche Wohnen	1	0.0320	1,438	14500	1.0086	13,665	437,280	30
	25	**-0.0096**	**38,235**	**16796**	**0.1462**	**81,313**	**1,177,602**	**28,901**

† Revenue of fiscal year prior to the event (consistent with GPDR penalties). Currencies converted based on rate at time of event.

‡ Current market capitalisation (Feb-21). Currencies converted based on rate at 31/12/2019.

Noting that of the top four negative CAAR events in **Table 2**, three of them are related to electricity companies it would certainly be interesting to look at industry sector analysis as recommended by e.g. Tweneboah-Kodua et al. (2018). A breakdown by sector is shown in **Table 3**. Here it can be seen that the most reactive industry sector was *Consumer Cyclical* (-1.5%), however, only *Utilities, Communication Services* and *Financial Services* showed statistical significance of non-zero (negative) abnormal returns albeit only at the 10% level.

Table 3: CAAR by industry sector

Industry Sector	N	CAAR	t_{CAAR}		% Negative CAR
Consumer Cyclical	2	-0.0148	-2.9208		100
Utilities	6	-0.0138	-2.1852	*	67
Energy	1	-0.0123			100
Communication Services	7	-0.0109	-2.1098	*	86
Industrials	3	-0.0092	-0.8761		33
Financial Services	5	-0.0086	-2.1881	*	100
Real Estate	1	0.0320	-2.0190		0
	25	**-0.0096**			**76**

* Represents statistical significance at the 10% level.

During the data collection exercise, it was noted that some of the larger GDPR fines had been appealed and the results of the appeals formally announced. This enabled an additional data set to be built (**Table 4**) and analysed in the same way as the initial announcements.

Table 4: Summary of GDPR fine appeals

Ultimate Parent	Date	Original fine	Result of appeal
Alphabet Inc	12/06/2020	€50m	Rejected
International Airlines	16/10/2020	£190m	Reduced to £20m
Marriott	30/10/2020	£99.2m	Reduced to £18.4m
United Internet	12/11/2020	€9.55m	Reduced to €900k

The expected outcome of these appeal announcements would be negative market price impact for the unsuccessful appeal by Alphabet Inc and positive for the other three examples where the fines were massively reduced. The results are shown in **Table 5**. It appears there is indeed, a negative trend for Alphabet beginning on the announcement day itself and not disappearing until 20 days after the event. International Airlines has a strongly increasing positive return after the event whereas, although positive, United Internet remains fairly constant. Marriott however, experienced some negative market sentiment after the event. One has to be mindful of market conditions and volatility due to the COVID-19 pandemic and its effect on (especially the hospitality) industry here. That was the reason the original data set was capped at 31/12/2019 and, in analysing these more recent events, the results were not found to be statistical significant thus the null hypothesis of zero abnormal returns still stands.

Table 5: CAR by event window of fines appealed

Event		Alphabet Inc		International Airlines		Marriott		United Internet	
Window	N	CAR	t_{CAR}	CAR	t_{CAR}	CAR	t_{CAR}	CAR	t_{CAR}
(-2, 2)	1	0.0164	0.5686	0.1459	1.1842	0.0455	0.7426	0.1039	1.9689
(-1, 1)	1	0.0026	0.1164	0.0499	0.5229	0.0143	0.3013	0.0563	1.3715
(-1, 0)	1	0.0054	0.2960	-0.0110	-0.1412	0.0346	0.8929	0.0431	1.2859
(0, 1)	1	-0.0076	-0.4166	0.0345	0.4427	-0.0045	-0.1179	0.0598	1.7917
(0, 2)	1	-0.0075	-0.3357	0.1059	1.1096	-0.0009	-0.0192	0.0812	1.9865
(0, 3)	1	-0.0008	-0.0310	0.0899	0.8158	-0.0187	-0.3463	0.0839	1.7775
(0, 4)	1	-0.0148	-0.5131	0.1349	1.0949	-0.0230	-0.3810	0.0753	1.4269
(0, 5)	1	-0.0171	-0.5412	0.1523	1.1284	0.0073	0.1104	0.0796	1.3770
(0, 10)	1	-0.0379	-0.8858	0.1596	0.8733	0.1250	1.3959	0.0827	1.0566
(0, 20)	1	0.0160	0.2707	0.3824	1.5145	0.1686	1.3626	0.0902	0.8340

5. Conclusion

We have seen how the announcement of monetary penalties related to GDPR infringement can result in (statistically significant) negative CARs of around 1% up to three days after the event. It was also observed that the economic impact on the market value of a publicly listed firm far outweighs the monetary value of the fine itself in almost all cases, and that a very small fine can have huge impact on market value (cf. BNP Paribas). We also know from the literature that CARs of a similar magnitude are generated at the time of the initial announcement of a breach. Considering all of these negative factors, the need for firms to invest in cyber security to protect data privacy is clearly underpinned by this research, as well as showing a clear economic impact of the introduction of the GDPR itself.

In light of the recent introduction of the GDPR, the dataset for this study was (necessarily) limited. Once more data becomes available and the market recovers from the COVID-19 pandemic, future research is expected to give a better idea of the impact of GDPR infringement fines on publicly listed firm value. Although four examples of GDPR fine appeals were identified and positive returns were observed where those appeals were successful (and the reverse), the results were not statistically significant, and we were unable to reject the null hypothesis of zero abnormal returns. Future research is needed in this area also – recently there has been news of Deutsche Wohnen appealing their €14.5m fine and, with the high-profile reductions of the fines for International Airlines (BA) and Marriott, a precedent appears to have been set with the ICO recognising and encouraging infringing firms to invest in cyber security measures (Macfarlanes 2020). Future studies may, therefore, reveal more about the positive impact of the GDPR on cyber security investment following its introduction and subsequent punitive actions. In this study only 2 out of 21 (10%) of ultimate parent firms were US based with the balance being European, therefore this work also begins to offset the strong US bias of these type of studies in the literature.

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

BBC (2013), *Sony fined over 'preventable' PlayStation data hack*, https://www.bbc.co.uk/news/technology-21160818. Accessed on: 30/03/2021

BBC (2016), *TalkTalk fined £400,000 for theft of customer details*, https://www.bbc.co.uk/news/business-37565367. Accessed on: 26/04/2021

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/. Accessed on: 26/02/2021

Daly A. (2018), *The introduction of data breach notification legislation in Australia: A comparative view*, Computer Law & Security Review, **34**, 477–495

Data Protection Act (1998), https://www.legislation.gov.uk/ukpga/1998/29/contents. Accessed on: 30/04/2021

Data Protection Act (2018), http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted. Accessed on: 10/03/2019

Data Protection Directive (1995), https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri= CELEX:31995L0046: en:HTML. Accessed on: 30/04/21

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)

ENISA (2020), *ETL2020 The Year in Review*, https://www.enisa.europa.eu/publications/year-in-review

European Commission (2021), *Proposal for an ePrivacy Regulation*, https://digital-strategy.ec.europa.eu/en/policies/eprivacy-regulation

European Convention on Human Rights (1950), https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/005. Accessed on: 30/04/21

Fama, E. F. (1970), *Efficient Capital Markets: A Review of Theory and Empirical Work*, The Journal of Finance, **25**(2), 383–417

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

Macfarlanes (2020), https://www.macfarlanes.com/what-we-think/in-depth/2020/lessons-from-the-ico-s-decisions-to-reduce-the-ba-and-marriott-gdpr-fines/. Accessed on: 26/02/21

MacKinlay, A. C. (1997), *Event Studies in Economics and Finance*, Journal of Economic Literature **35**(1) (March)

Murciano-Goroff (2019), *Do Data Breach Disclosure Laws Increase Firms' Investment in Securing Their Digital Infrastructure?,* WEIS 2019

Nieuwesteeg, B., Faure, M. (2018), *An analysis of the effectiveness of the EU data breach notification obligation*, Computer Law & Security Review: **34**(6), 1232-1246

Privacy and Electronic Communications Directive (2002), https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058. Accessed on: 30/04/21

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

Romanosky, S., Telang, R., Acquisti, A. (2011), *Do Data Breach Disclosure Laws Reduce Identity Theft?*, Journal of Policy Analysis and Management, **30**(2), 256-286

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

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

Yahoo!Finance (2019), *Historical Data*, https://finance.yahoo.com/quote