Finance Research Letters 71 (2025) 106361

Contents lists available at ScienceDirect

Finance Research Letters

journal homepage: www.elsevier.com/locate/frl

Stock-Term market impact of major cyber-attacks: Evidence for the ten most exposed insurance firms to cyber risk

António Miguel Martins [a,b], Nuno Moutinho [c,d,*]

[a] University of Madeira - Faculty of Social Sciences, Caminho da Penteada, 9020-105 Funchal, Portugal
[b] Centre of Applied Economic Studies of the Atlantic (CEEAplA), Ponta Delgada, Azores, Portugal
[c] Instituto Politécnico de Bragança, Campus de Santa Apolónia, 5300-253 Bragança, Portugal
[d] Unidade de Investigação Aplicada em Gestão (UNIAG), Portugal

ARTICLE INFO

Keywords:
Insurance
Cyberattack
Cyber risk
Market reaction
Event study

ABSTRACT

The main focus of this paper is to study empirically the impact of major cyberattacks in the market value of the ten most exposed insurers to cyber risk. Using an event study for 53 global cyberattacks, we observe a negative and statistically significant stock price reaction for insurers around the cyberattack disclosure dates. The increase in the assessed probability of an increase in future payments tends to prevail over the increase in demand and/or premiums caused by the disclosure of global major cyberattacks. The results of our analysis also show a higher negative stock market reaction for small insurers and when involves financial information loss.

1. Introduction

In a world plagued by escalating cyber threats, businesses must prioritize cyber security like never before. Some alarming statistics on the impact of cyberattacks emphasize the need for robust security solutions. Recent data reveals a nearly 50 % increase in cyber extortion in 2023, and a surprising 1 in 10 organizations worldwide to be hit by attempted ransomware attacks – a 33 % jump from the previous year (Allianz 2024). A widely accepted notion goes that there are only two types of firms: those that have been breached and those that don't know they have (Kvochko and Pant, 2015).

According to Cybercrime Magazine (2020), cybercrime has inflicted losses totalling $6 trillion USD and it is expected a grow of cybercrime costs by 15 percent per year over the next years, reaching $10,5 trillion USD annually in 2025. If cybercrime were measured as a country, then it would be the third largest economy in the world after the US and China. Cybercrime will eventually be more profitable than the global trade of all major illegal drugs combined (Cybercrime Magazine 2020).

Cyberattacks impose direct and indirect costs on firms that see their privacy violated (e.g., Cavusoglu et al., 2004; Arcuri et al., 2018; Corbet and Gurdgiev, 2019; Kamiya et al., 2021). These costs include lower sales revenue and decreased productivity resulting from the unavailability of the breached resources, loss of funds or customer records, litigation costs, labour and material costs required to detect, contain, repair, and reconstitute breached resources. Moreover, attacked firms experience a decrease in credit ratings (e.g., Kamiya et al., 2021). All this evidence is consistent with the existence of a reputation loss for target firms. Kamiya et al. (2021) demonstrate that successful cyberattacks have economically large reputation costs in that the shareholder wealth loss far exceeds the out-of-pocket costs from the attack.

* Corresponding author.
E-mail addresses: antonio.martins@staff.uma.pt (A.M. Martins), nmoutinho@ipb.pt (N. Moutinho).

https://doi.org/10.1016/j.frl.2024.106361
Received 28 July 2024; Received in revised form 4 October 2024; Accepted 25 October 2024
Available online 5 November 2024
1544-6123/© 2024 Elsevier Inc. All rights are reserved, including those for text and data mining, AI training, and similar technologies.

Cyber risk can also affect insurance firms in two different ways (Eling and Schnell, 2016). First, as they rely critically on their IT infrastructure, they are highly vulnerable to cyber risk. This exposure is treated by regulatory frameworks as part of the operational risk category (operational cyber risk). Second, for its cyber risk underwriting policies (underwriting cyber risk). One of the arguments often put forward as an explanation for the absence of significant returns around the announcement of a cyberattack is that insurance firms absorb a substantial amount of the direct costs associated with the cyberattack (Haislip et al., 2019).

However, there are several authors who have illustrated the immense difficulties to insure cyber risk (e.g., Biener et al., 2015; Eling and Schnell, 2016; PWC, 2018). According to Biener et al. (2015) the three major insurability problems of cyber risk are as follows: (*i*) the independence and predictability of losses are not given; thus, the risk pooling might not always work appropriately; (*ii*) information asymmetry – firms that have experienced a cyberattack are most likely to buy insurance (e.g., Shackelford, 2012), thus resulting in adverse selection. In addition, there is moral hazard, i.e., the change of behaviour after purchasing insurance. One example is the insured's reduced incentive to invest in self-protection measures following the purchase of insurance if full coverage is offered; (*iii*) the existing policies only cover small losses and contain several exclusions. Potential extreme scenarios can thus not be well covered by existing insurance policies. Given the large number of exclusions and the dynamic nature of cyber risk, there is uncertainty about what the cyber policy actually covers.

So overall, the available policies do not really cover what the supply side is looking for efficient protection not for the small risks, but for the extreme cases which might lead to big losses. Even so, a recent report on the cyber insurance market size reveals that this market is worth USD 16.66 billion in 2023 (Fortune Business Insights, 2024). The market is projected to grow from USD 20.88 billion in 2024 to USD 120.47 billion by 2032, exhibiting a compound annual growth rate of 24.5 % during the forecast period.

Despite its increasing relevance for business at present, the empirical studies that investigate the stock price reaction to cyber-attacks are scarce and are mainly focused on the analysis of breached firms by a cyberattack, with Ettredge and Richardson (2003), Cavusoglu et al. (2004), Arcuri et al. (2018), Tosun (2021) finding evidence of a significant effect on stock prices, while Campbell et al. (2003), Hovav and D'Arcy (2003), Kannan et al. (2007) do not find any statistically significant impact on the market value of firms. Finally, Kamiya et al. (2021) find that cyberattacks that do not involve the loss of personal financial information do not cause a significant shareholder loss. In contrast, cyberattacks where personal financial information is lost involve a significant shareholder wealth loss.

Other empirical studies have also examined the effect of cyberattacks on non-breached industry peers, auditors, and affected insurers (Haislip et al., 2019) and on industry competitors (Kamiya et al., 2021). Both studies find that non-breached competitors experience significant negative equity returns around the announcement of a cybersecurity breach in their industry. Haislip et al. (2019) also find a material increase in audit fees during the year of the infraction and significant negative equity returns for insurers with material cybersecurity exposure.

We contribute to the literature by examining the impact caused by the largest global cyberattacks in the ten most exposed insurers to cyber risk. The present study differs from Haislip et al. (2019)'s study due to the fact that it focuses only on insurers with a higher exposure to cyber risk (and not on all listed insurers) and the analysis of the major global cyberattacks over the period 2010 to 2023, instead of all the cyberattacks between 2010 and 2018. To the best of our knowledge, this is the first study which focuses only on the impact of major cyberattacks on the main exposed insurers to cyber risk. We choose the largest insurers since they are the most informed about the cyber security market and have the greatest ability to anticipate the risk of future cyber-attacks in their clients (Florackis et al., 2023; Jiang et al., 2024). This study adds information on the spillover effects of target firms cyberattacks on insurers, the most relevant stakeholders to protect and minimize the firm's loss from that adverse event. This paper also extends the results of Eckert et al. (2023) by incorporating the effects of firm's financial information loss on insurers' market reaction.

Using an event study methodology for a sample of 53 global cyberattacks, we observe a negative and statistically significant stock price reaction for insurers around the cyberattack disclosure date. Our results also show a highest negative stock market reaction for small insurers and when involves financial information loss.

2. Impact of cyberattacks on market value of insurers

Cyberattacks seems to have a negative impact on the abnormal returns of target firms when attacks are announced (Hogan et al., 2023; Kamiya et al., 2021). Additionally, these effects can spillover to other firms within the same industry (Baldwin et al., 2017; Tosun, 2021) and even to firms in other industries (Eckert et al., 2020, 2023). This spillover effect is the sum of two contradictory effects: the competitive effect refers to a benefit or positive effect on non-attacked firms, while the contagion effect implies that non-attacked firms also experience financial loss (Lang and Stulz, 1992). The spillover effect may also impact insurers, for example through operational risk events, insurance premium, or insurance loss (e.g., Eckert et al., 2020).

The impact of cyberattacks on insurers is difficult to predict in advance, given that there are opposing forces in play. On the one hand, the disclosure of a cyberattack may positively affect the insurers as demand for cyber insurance and/or premia charged is likely to increase. As mentioned previously, firms that have experienced a serious cyberattack are most likely to buy insurance (Shackelford, 2012). Added to this is the strong appetite among underwriters for further expansion in cyber insurances writings, reflecting what would appear to be favourable prices in comparison to other areas of a generally soft market – the cost of cyber insurance relative to the limit purchased is typically three times the cost of cover for more established general liability risks (PWC, 2018). On the other hand, the disclosure of a cyberattack triggers a policy payout and may increase the assessed probability of an increase in future payouts as more firms are breached. Chen et al. (2012) appeal to similar arguments in their study of the impact of cyberattacks on IT consultants. Additionally, insurers tend to suffer from moral hazard problems, as firms tend to change their behaviour after purchasing insurance (e.g., Biener et al., 2015). As a result, insured firms see their incentive to invest in self-protection measures following the purchase of

insurance if full coverage is offered. This fact tends to contribute to an increase in future payouts paid by insurers.

The first effect implies a positive stock market reaction for insurers around the revelation of a material cyberattack (competitive effect), while the latter implies a negative stock market reaction (contagion effect). The main objective of the present study is to know which of the forces dominates, i.e., whether the net effect is positive, negative or zero. Therefore, our research hypothesis is the following:

Null Hypothesis (H_0): A cyberattack disclosure does not affect the short-term market value of cybersecurity insurance providers.

Finally, we also analyse whether the size of the insurer and the type of information lost influence the abnormal returns found around cyberattack disclosures. The financial literature shows that size affects the firm's market power advantage, economies of scale, and financial performance in the end. Titman and Wessels (1988) refer that large firms tend to diversify their businesses more efficiently and are less prone to bankruptcy. In the context of insurance literature, large insurance firms are likely to be more diversified and are therefore better able to handle large losses (e.g., Chen et al., 2008). In turn, Kamiya et al. (2021), in their analysis for breached firms, they find that cyberattacks that do not involve the loss of personal financial information do not cause a significant shareholder wealth loss. In contrast, cyberattacks where personal financial information (e.g., loss of social security numbers and financial information such as credit card information) is lost involve a significant shareholder wealth loss. From this it is possible to conclude that the cost for insurers in the event of a cyberattack will tend to be higher in the case of attacks involving the loss of financial information.

3. Data and methodology

The data used in the event study is collected from different sources. We analyse the ten insurers with significant cybersecurity insurance exposure.[1] Haislip et al. (2019) identified the same list of insurers heavily exposed to cyber risk. Table 1 presents the list of the 10 insurance firms analysed in this study. Insurer' stock returns were obtained from Eikon Refinitiv. The list of major cyberattacks,[2] initially made up of 109 cyberattacks, was reduced to 53 announcements after we removed attacks on firms or organizations not publicly listed on the stock market. The list identifies the firms targeted by the attacks, the dates when cyberattacks were disclosed to the market, and the type of information breached, for a set of cyberattacks that occurred between 2010 and 2023. Table 2 presents the distribution of cyberattacks by country and industry.

To test the research hypothesis presented in the previous section, we employ the market model and the Fama-French (2015) five-factor models. The five factors of Fama and French (2015) were obtained from the homepage of Kenneth French at Dartmouth College.[3] We use the dates of market disclosure of cyberattacks as event dates to compute abnormal returns (ARs), which are obtained by the difference between observed returns of insurer firm i on day t and the expected return generated by the market model, as follows:

$$AR_{it} = R_{it} - E(R_{it}) \tag{1}$$

The event dates are designated as day $t = 0$. We use the window −10 days and −40 days to estimate the expected return on the event day. Usually, event studies geared to financial data employ an estimation window of roughly 30 to 100 days (Moser and Brauneis, 2023). The use of an extended estimation window, given the temporal proximity of some of the analysed events, could lead to overlapping event situations. To prevent this from happening we use an estimating window of 30 days. Similar procedure was adopted by Martins (2024). The benchmark index used to calculate the abnormal returns was the daily return of the market index of the country of each insurer firm. Fig. 1 presents the event timeline used to calculate the abnormal returns. By cumulating the ARs over a particular time interval, we obtain the cumulative abnormal returns (CARs) as follows:

$$CAR[t_1, t_2] = \sum_{t_1}^{t_2} AR_t \tag{2}$$

Four different time intervals for the CARs were considered: [−1,1], [−1,2], [−1,5] and [−1,10]. Finally, we calculate the cumulative average abnormal returns (CAARs) for each time intervals as follows:

$$CAAR[t_1, t_2] = 1 \Big/ N \sum_{t_1}^{t_2} CAR_{[t1,t2]} \tag{3}$$

where, N is the sample size of the group.

Finally, in the analysis of abnormal returns differences between insurers based on the size and type of information loss, we calculate the CAARs and their differences for each portfolio. The analysis of the statistical significance of the differences obtained for the portfolios is carried out based on a two-sample t-test.

[1] Information about each insurer is available here: https://cybermagazine.com/top10/top-10-cyber-insurance-companies.
[2] The list can be found here: https://termly.io/resources/articles/biggest-data-breaches/.
[3] https://mba.tuck.dartmouth.edu/pages/faculty/ken.french/data_library.html.

Table 1
List of the Ten Major Global Cyber Insurance Firms.
This table presents the list of the ten major global cyber insurance, their market capitalization on December 31, 2023 (thousands of USD), and the country where they have their headquarters. The list was constructed with information obtained here: https://cybermagazine.com/top10/top-10-cyber-insurance-companies.

Insurance Firm	Market Capitalization	Country
AXA	107 207 000	France
Chubb	72 542 000	Switzerland
American International Group (AIG)	67 488 000	USA
Zurich Insurance Group AG	38 350 000	Switzerland
Munich *Re*	34 362 000	Germany
The Travelers Companies	32 852 000	USA
The Hartford Financial Services Group	19 689 000	USA
AXIS Capital Holdings Limited	6 662 700	Bermuda
Beazley plc	4 430 400	UK
Hiscox Ltd	3 962 600	Bermuda

Table 2
Distribution of Cyberattacks by Country and Industry.
This table presents the 53 major cyberattacks over the period 2010 to 2023 by country and industry.

Country	#	Country	#
AUSTRALIA	2	SOUTH KOREA	1
BRAZIL	1	TURKEY	1
CHINA	2	UK	2
IRELAND	1	USA	40
JAPAN	3		
Industry	#	**Industry**	#
Communication Services	8	Finance Services	7
Consumer Cyclical – Internet Retail	5	Healthcare	4
Consumer Cyclical – Leisure, Lodging, Resort and Casinos	5	Industrials	4
Consumer Cyclical – Apparel, Home and Auto	5	Technology	12
Consumer Defensive	3		

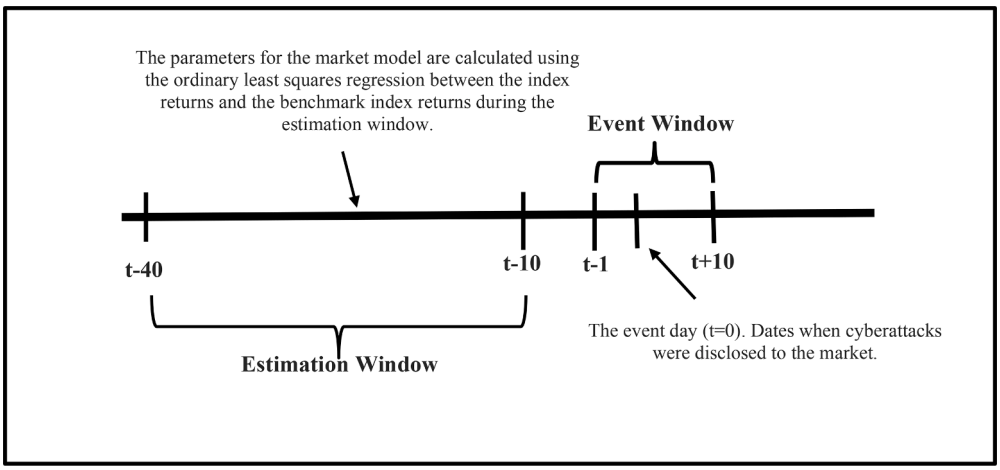

Fig. 1. Event Timeline.
The figure presents the event timeline used to calculate the abnormal returns for the ten major global cyber insurance, based on the 53 major global cyberattacks over the period 2010 to 2023.

Table 3
Cumulative Average Abnormal Returns (CAARs) by Cyber Insurance Firm.
This table presents the CAARs for the ten major global cyber insurance calculated using market model (*MM*) and Fama-French five-factor model (*FF5*), based on the 53 major global cyberattacks over the period 2010 to 2023, for four different time windows: [−1;+1]; [−1;+2]; [−1;+5] and [−1,+10]. At the end of the table, the CAAR for ten major global cyber insurance (entire sample) is also presented. θ_1 and τ_1 are the *p-values* of Brown and Warner (1980, 1985) *t*-test statistics and *z*-statistic for the sign test, respectively (see Serra, 2004, for more details). *, ** and *** denote statistical significance at the 10 %, 5 % and 1 % level, respectively.

	Cyber Insurance Firm		**Market Model (MM)**			
			[−1;1]	**[−1;2]**	**[−1;5]**	**[−1;10]**
1	AXA	CAAR	−0.34 %	−0.86 %	−1.09 %	−0.85 %
		θ_1	0.059*	0.018**	0.040**	0.059*
		τ_1	0.061*	0.019**	0.041**	0.062*
2	Chubb	CAAR	−0.30 %	−0.79 %	−0.83 %	−0.92 %
		θ_1	0.065*	0.021**	0.053*	0.049**
		τ_1	0.067*	0.022**	0.053*	0.050**
3	AIG	CAAR	−0.26 %	−0.70 %	−0.87 %	−0.94 %
		θ_1	0.069*	0.028**	0.046**	0.047**
		τ_1	0.070*	0.029**	0.048**	0.048**
4	Zurich Insurance Group	CAAR	−0.24 %	−0.86 %	−0.62 %	−0.95 %
		θ_1	0.074*	0.019**	0.065*	0.045**
		τ_1	0.077*	0.020**	0.067*	0.046**
5	Munich *Re*	CAAR	−0.40 %	−0.84 %	−0.94 %	−1.26 %
		θ_1	0.046**	0.020**	0.045**	0.039**
		τ_1	0.048**	0.022**	0.046**	0.037**
6	The Travelers Companies	CAAR	−0.81 %	−0.88 %	−0.98 %	−1.42 %
		θ_1	0.013**	0.022**	0.041**	0.021**
		τ_1	0.014**	0.023**	0.042**	0.020**
7	The Hartford Financial Services Group	CAAR	−0.85 %	−1.04 %	−1.01 %	−1.55 %
		θ_1	0.011**	0.018**	0.040**	0.018**
		τ_1	0.012**	0.019**	0.041**	0.019**
8	AXIS Capital Holdings Limited	CAAR	−0.90 %	−1.03 %	−1.39 %	−1.01 %
		θ_1	0.011**	0.018**	0.034**	0.042**
		τ_1	0.013**	0.018**	0.035**	0.042**
9	Beazley plc	CAAR	−1.43 %	−1.92 %	−2.62 %	−1.69 %
		θ_1	0.007***	0.009***	0.012**	0.016**
		τ_1	0.008***	0.010***	0.013**	0.018**
10	Hiscox Ltd	CAAR	−0.37 %	−0.81 %	−0.84 %	−2.15 %
		θ_1	0.051*	0.023**	0.049**	0.009***
		τ_1	0.052*	0.024**	0.051*	0.009***
All Sample		CAAR	−0.59 %	−0.97 %	−1.12 %	−1.27 %
		θ_1	0.034**	0.021**	0.039**	0.038**
		τ_1	0.036**	0.022**	0.040**	0.038**
	Cyber Insurance Firm		Fama-French Five-Factor Model (FF5)			
			[-1;1]	[-1;2]	[-1;5]	[-1;10]
1	AXA	CAAR	−0.23 %	−0.72 %	−0.98 %	−1.45 %
		θ_1	0.080*	0.025**	0.039**	0.025**
		τ_1	0.079*	0.028**	0.041**	0.028**
2	Chubb	CAAR	−0.23 %	−0.44 %	−0.79 %	−1.20 %
		θ_1	0.082*	0.090*	0.057*	0.039**
		τ_1	0.081*	0.093*	0.059*	0.041**
3	AIG	CAAR	−0.70 %	−1.16 %	−0.70 %	−1.59 %
		θ_1	0.018**	0.015**	0.062*	0.017**
		τ_1	0.020**	0.017**	0.066*	0.018**
4	Zurich Insurance Group	CAAR	−0.32 %	−0.91 %	−0.76 %	−0.94 %
		θ_1	0.061*	0.021**	0.056*	0.045**
		τ_1	0.060*	0.020**	0.053*	0.045**
5	Munich *Re*	CAAR	−0.48 %	−0.78 %	−0.90 %	−0.93 %
		θ_1	0.042**	0.022**	0.042**	0.043**
		τ_1	0.044**	0.025**	0.041**	0.045**
6	The Travelers Companies	CAAR	−0.37 %	−0.96 %	−1.35 %	−1.03 %
		θ_1	0.048**	0.020**	0.033**	0.040**
		τ_1	0.047**	0.019**	0.034**	0.039**
7	The Hartford Financial Services Group	CAAR	−0.67 %	−1.25 %	−1.31 %	−1.61 %
		θ_1	0.019**	0.015**	0.035**	0.015**
		τ_1	0.020**	0.015**	0.033**	0.017**
8	AXIS Capital Holdings Limited	CAAR	−0.80 %	−0.99 %	−1.32 %	−1.28 %
		θ_1	0.014**	0.017**	0.035**	0.037**
		τ_1	0.016**	0.018**	0.033**	0.039**
9	Beazley plc	CAAR	−1.23 %	−2.35 %	−2.21 %	−1.40 %

(*continued on next page*)

Table 3 (*continued*)

	Cyber Insurance Firm		Fama-French Five-Factor Model (FF5)			
			[-1;1]	[-1;2]	[-1;5]	[-1;10]
		θ_1	0.008***	0.008***	0.015**	0.021**
		τ_1	0.009***	0.007***	0.017**	0.023**
10	Hiscox Ltd	CAAR	−0.25 %	−0.68 %	−0.98 %	−1.59 %
		θ_1	0.071*	0.029**	0.040**	0.017**
		τ_1	0.074*	0.031**	0.039**	0.019**
All Sample		CAAR	−0.53 %	−1.02 %	−1.13 %	−1.30 %
		θ_1	0.036**	0.019**	0.039**	0.037**
		τ_1	0.037**	0.020**	0.039**	0.038**

4. Results

4.1. Abnormal returns

Table 3 presents the CAARs observed for the ten insurers around the major global cyberattack disclosure dates. We observe a negative and statistically significant stock price reaction around these event dates. The CAARs for the total sample are also negative and statistically significant. The parametric and non-parametric tests[4] show that there is a level of statistical significance of 5 % for the four-time intervals. The cumulative average abnormal return (CAAR) is −0.59 % (market model) and −0.53 % (Fama-French five-factor model) during the three-day window around cyberattack announcements. The present results show that the policy payouts triggered by major global cyberattacks, as well as the revised assessment of expected future payouts, outweigh the potential increase in revenue. These results reinforce the idea already confirmed in other studies (e.g., Cavusoglu et al., 2004; Haislip et al. 2019; Kamiya et al., 2021; Eckert et al., 2020 and 2023) that the costs from cyberattacks extend well beyond the breached firm itself, suggesting the dominance of contagion effects. Finally, these results provide evidence in support of the claim that insurers absorb the impact in terms of costs caused by cyberattacks (e.g., Eling and Schnell, 2016; PWC, 2018), adding a piece to the puzzle of investors' apparent disinterest in the disclosure of the information at the breached firm. These results for insurers may be related to operational risk events (Eckert et al., 2020), the possibility for other similar events in the future, along with reputation damage (Cummins et al., 2007; Foerderer and Schuetz, 2022), sine cyberattacks attract negative attention and damage future prospects, costs and uncertainty (Tosun, 2021). Additionally, also cyberattacks can undermine investor confidence in insurers' ability to adequately assess cyber risk (Shandler and Gomez, 2023) and create a high uncertainty environment, leading to negative market sentiment. Since we study major cyberattacks, the negative investor sentiment will be higher due to extensive media coverage (Foerderer and Schuetz, 2022).

We also perform a difference of means test between the observed CAARs for the ten insurer firms, in terms of size and type of information lost, for the four-time windows. Table 4 presents the CAARs obtained for each of the portfolios as well as the results of the two-sample *t*-test for differences in the abnormal returns. The results show a lower negative abnormal return for larger insurer firms and when the cyberattack not involve financial information loss. Large insurance firms are likely to be more diversified and are therefore better able to handle large losses (e.g., Chen et al., 2008). Finally, cyberattacks that result in financial information loss tend to cause greater shareholder wealth loss in breached firms (e.g., Kamiya et al., 2021), which tends to lead to the payment of higher policy payouts by insurance firms.

4.2. Abnormal returns robustness checks

We conduct two additional robustness checks to assess the sensitivity of our findings to the length of estimation window and alternative benchmarks. For the first purpose, abnormal returns were calculated using a wider estimation window. Although the literature shows that the length of the estimation window does not tend to significantly affect the magnitude of abnormal returns (e.g., Park 2004; Sorescu et al., 2017), these authors agree that it must be ensured that the results are not unduly affected by outliers or unusual movements, that are more likely to create noise in shorter estimation windows. Therefore, abnormal returns were estimated using an estimation window of 220 trading days as in Kamiya et al. (2021) and Eckert et al. (2023). The general conclusions of the study did not change when the estimation period is extended. Finally, we analyze the robustness of abnormal returns using an alternative benchmark (an industry-specific index) – S&P Insurance Select Industry Index.[5] The general conclusions remain valid when this alternative benchmark is used. Due to space limitations, the results of both robustness checks are available upon request from the authors.

5. Concluding remarks

This paper analyses the short-term market impact of 53 major global cyberattacks in the market value of the ten most exposed

[4] For more details, please see Serra (2004).
[5] https://www.spglobal.com/spdji/en/indices/equity/sp-insurance-select-industry-index/.

Table 4
CAARs for Cyber Insurance Firms and Cumulative Average Abnormal Returns Differences for Firm Size and Type of Information Loss.
This table presents the CAARs for the ten major global cyber insurance calculated around the53 major global cyberattacks announcement dates, calculated using market model (*MM*) and Fama-French five-factor model (*FF5*), and the differences in terms of cybersecurity firms' CAARs across different subsamples of firm size (Panel 1) and type of information loss (Panel 2), for four different time windows: [−1;+1]; [−1;+2]; [−1;+5] and [−1,+10]. θ_1 and τ_1 are the *p-values* of Brown and Warner (1980, 1985) *t*-test statistics and *z*-statistic for the sign test, respectively (see Serra, 2004, for more details). The significance of the differences in CAARs is determined via two-sample *t*-test. *, ** and *** denote statistical significance at the 10 %, 5 % and 1 % level, respectively.

			[−1;1]	**[−1;2]**	**[−1;5]**	**[−1;10]**
Panel 1: Difference in the CAARs Across Different Cyber Insurance Firm's Size						
Market Model (*MM*)						
Above the Sample Median	5	CAAR	−0.308 %	−0.810 %	−0.870 %	−0.983 %
		θ_1	0.048**	0.022**	0.040**	0.042**
		τ_1	0.049**	0.024**	0.041**	0.043**
Below the Sample Median	5	CAAR	−0.871 %	−1.134 %	−1.369 %	−1.563 %
		θ_1	0.010***	0.015**	0.020**	0.017**
		τ_1	0.011**	0.016**	0.021**	0.018**
Difference		CAAR *t*-test *(p-value)*	0.563 %	0.324 %	0.498 %	0.579 %
			0.012**	0.035**	0.037**	0.036**
Fama-French Five-Factor Model (*FF5*)						
Above the Sample Median	5	CAAR	−0.378 %	−0.756 %	−0.872 %	−0.979 %
		θ_1	0.036**	0.028**	0.041**	0.043**
		τ_1	0.039**	0.030**	0.042**	0.044**
Below the Sample Median	5	CAAR	−0.677 %	−1.294 %	−1.391 %	−1.451 %
		θ_1	0.027**	0.012**	0.019**	0.021**
		τ_1	0.029**	0.013**	0.018**	0.023**
Difference		CAAR *t*-test *(p-value)*	0.299 %	0.538 %	0.519 %	0.472 %
			0.042**	0.016**	0.031**	0.045**
			[−1;1]	**[−1;2]**	**[−1;5]**	**[−1;10]**
Panel 2: Difference in the CAARs Across Different Type of Information Loss						
Market Model (*MM*)						
	# Cyberattacks					
Financial Information Loss	10	CAAR	−1.407 %	−1.192 %	−1.188 %	−1.479 %
		θ_1	0.006***	0.012**	0.019**	0.017**
		τ_1	0.006***	0.012**	0.020**	0.018**
Other Information Loss	43	CAAR	0.024 %	0.230 %	0.294 %	0.738 %
		θ_1	0.423	0.311	0.378	0.080*
		τ_1	0.431	0.315	0.385	0.082*
Difference		CAAR *t*-test *(p-value)*	−1.431 %	−1.422 %	−1.482 %	−2.217 %
			0.000***	0.003***	0.004***	0.003***
Fama-French Five-Factor Model (*FF5*)						
Financial Information Loss	10	CAAR	−1.482 %	−1.255 %	−1.208 %	−1.486 %
		θ_1	0.005***	0.011**	0.016**	0.016**
		τ_1	0.006***	0.013**	0.018**	0.017**
Other Information Loss	43	CAAR	0.224 %	0.396 %	0.344 %	0.770 %
		θ_1	0.388	0.277	0.341	0.077*
		τ_1	0.391	0.283	0.335	0.079*
Difference		CAAR *t*-test *(p-value)*	−1.706 %	−1.651 %	−1.552 %	−2.256 %
			0.000***	0.001***	0.002***	0.003***

insurers to cyber risk. The results show a negative and statistically significant stock price reaction for insurers around the cyberattack disclosure date. We may conclude that there is a dominance of contagion effects over the competitive effect. Our results also show that the abnormal returns observed for insurers around the cyberattack disclosure dates tend to be higher for small size insurance firms and when they involve financial information loss.

As mentioned before, these results provide evidence in support of the claim that insurers absorb the impact in terms of costs caused by cyberattacks (e.g., Eling and Schnell, 2016; PWC, 2018). Despite the strong growth trend in the cyber risk business for insurance firms, these results show the need for a more informed and sustainable cyber insurance model, in order to allow a more efficient allocation of capital, an efficient reinsurance market and capital market risk transfer. These factors are fundamental in capitalizing on the benefits of the increasing digitalization of the economy.

Insurance firms' enhanced ability to comprehensively assess the ex-ante risk of cyberattacks (Jiang et al., 2024; Florackis et al., 2023), should lead to improved risk analysis of their clients. This, in turn, will enable them to steer clear of high-risk clients that could significantly impact the insurers' market prices or to adjust insurance premiums based on the likelihood of such events occurring.

With respect to practical implications, research suggests that managers and chief information officers with IT expertise are less

likely to experience cyberattacks (Kamiya et al., 2021), and firms in technological sectors that provide more information about cyberattacks to the market tend to experience less negative abnormal returns (Amir et al., 2018). In light of this evidence, it is recommended that market regulators require insurers to disclose more information on IT security and data breaches, as well as disclose those responsible for these issues and their position on the firm's board.

Regarding future research, we suggest an analysis of the impact of cyberattacks on smaller insurers that may have less access to information and lower ability to anticipate the risk of future cyberattacks.

CRediT authorship contribution statement

António Miguel Martins: Conceptualization, Methodology, Formal analysis, Software, Writing – review & editing. **Nuno Moutinho:** Writing – original draft, Project administration, Methodology, Investigation, Funding acquisition, Formal analysis.

Declaration of competing interest

None.

Acknowledgement

This paper is financed by Portuguese national funds through FCT – Fundação para a Ciência e a Tecnologia, I.P., projects numbers UIDB/00685/2020 (António Martins) and UNIAG, UIDB/04752/2020 and UIDP/04752/2020 (Nuno Moutinho).

Data availability

Data will be made available on request.

References

Allianz (2024). Cyber-Attaks are good for business – If your business is cyber security. Available here: https://www.allianzgi.com/en/insights/two-minute-tech/cyber-attacks-are-good-for-business-if-your-business-is-cyber-security. Accessed on June 5, 2024.
Amir, E., Levi, S., Livne, T., 2018. Do firms underreport information on cyber-attacks? Evidence from capital markets. Rev. Account. Stud. 23, 1177–1206.
Arcuri, M.C., Brogi, M., Gandolfi, G., 2018. The effect of cyber-attacks on stock returns. Corp. Ownership Control 15 (2), 70–83.
Baldwin, A., Gheyas, I., Ioannidis, C., Pym, D., Williams, J., 2017. Contagion in cyber security attacks. J. Oper. Res. Soc. 68 (7), 780–791.
Biener, C., Eling, M., Wirfs, J.H., 2015. Insurability of cyber risk: an empirical analysis. Geneva Pap. Risk Insur.-Issues Pract. 40, 131–158.
Brown, S.J., Warner, J.B., 1980. Measuring security price performance. J. Financ. Econ. 8 (3), 205–258.
Brown, S.J., Warner, J.B., 1985. Using daily stock returns: the case of event studies. J. Financ. Econ. 14 (1), 3–31.
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. J. Comput. Secur. 11 (3), 431–448.
Cavusoglu, H., Mishra, B., Raghunathan, S., 2004. The effect of internet security breach announcements on market value: capital market reactions for breached firms and internet security developers. Int. J. Electron. Commerce 9 (1), 70–104.
Chen, J.V., Li, H.C., Yen, D.C., Bata, K.V., 2012. Did IT consulting firms gain when their clients were breached? Comput. Human. Behav. 28 (2), 456–464.
Chen, X., Doerpinghaus, H., Lin, B.X., Yu, T., 2008. Catastrophic losses and insurer profitability: evidence from 9/11. J. Risk Insur. 75 (1), 39–62.
Corbet, S., Gurdgiev, C., 2019. What the hack: systematic risk contagion from cyber events. Int. Rev. Financ. Anal. 65, 101386.
Cummins, J.D., Wei, R. and Xie, X. (2007). Financial sector integration and information spillovers: effects of operational risk events on US banks and insurers. *Available at SSRN 1071824*.
Cybercrime Magazine (2020). Cybercrime to cost the world $10.5 trillion annually by 2025. Available here: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/. Accessed on June 5, 2024.
Eckert, C., Gatzert, N., Heidinger, D, 2020. Empirically assessing and modeling spillover effects from operational risk events in the insurance industry. Insur. Math. Econ. 93, 72–83.
Eckert, C., Gatzert, N., Schubert, M., 2023. Analyzing spillover effects from data breaches to the US (Cyber) insurance industry. Eur. J. Finance 29 (6), 669–692.
Eling, M., Schnell, W., 2016. What do we know about cyber risk and cyber risk insurance? J. Risk Finance 17 (5), 474–491.
Ettredge, M.L., Richardson, V.J., 2003. Information transfer among internet firms: the case of hacker attacks. J. Inf. Syst. 17 (2), 71–82.
Fama, E.F., French, K.R., 2015. A five-factor asset pricing model. J. Financ. Econ. 116 (1), 1–22.
Florackis, C., Louca, C., Michaely, R., Weber, M., 2023. Cybersecurity risk. Rev. Financ. Stud. 36 (1), 351–407.
Foerderer, J., Schuetz, S.W., 2022. Data breach announcements and stock market reactions: a matter of timing? Manage. Sci. 68 (10), 7298–7322.
Fortune Business Insights (2024). Cyber insurance market size. Available here: https://www.fortunebusinessinsights.com/cyber-insurance-market-106287. Accessed on May 16, 2024.
Haislip, J., Kolev, K., Pinsker, R., Steffen, T., 2019. The economic cost of cybersecurity breaches: a broad-based analysis. In: Workshop on the Economics of Information Security (WEIS), pp. 1–37.
Hogan, K.M., Olson, G.T., Mills, J.D., Zaleski, P.A., 2023. An analysis of cyber breaches and effects on shareholder wealth. Int. J. Econ. Bus. 30 (1), 51–78.
Hovav, A., D'Arcy, J, 2003. The impact of denial-of-service attack announcements on the market value of firms. Risk. Manage. Insur. Rev. 6 (2), 97–121.
Jiang, H., Khanna, N., Yang, Q., Zhou, J., 2024. The cyber risk premium. Manage. Sci. https://doi.org/10.1287/mnsc.2022.02056.
Kamiya, S., Kang, J.K., Kim, J., Milidonis, A., Stulz, R.M., 2021. Risk management, firm reputation, and the impact of successful cyberattacks on target firms. J. Financ. Econ. 139 (3), 719–749.
Kannan, K., Rees, J., Sridhar, S., 2007. Market reactions to information security breach announcements: an empirical analysis. Int. J. Electron. Commerce 12 (1), 69–91.
Kvochko, E., Pant, R., 2015. Why data breaches don't hurt stock prices. Harv. Bus. Rev. 31, 2015.
Lang, L.H., Stulz, R., 1992. Contagion and competitive intra-industry effects of bankruptcy announcements: an empirical analysis. J. Financ. Econ. 32 (1), 45–60.
Martins, A.M., 2024. Short-Term market impact of crypto firms' bankruptcies on cryptocurrency markets. Res. Int. Bus. Finance 70, 102370.
Moser, S., Brauneis, A., 2023. Should you listen to crypto YouTubers? Financ. Res. Lett. 54, 103782.
Park, N.K., 2004. A guide to using event study methods in multi-country settings. Strateg. Manage J. 25 (7), 655–668.

PwC. 2018. Insurance 2020 & beyond: reaping the dividends of cyber resilience. Available at: https://www.pwc.com/gx/en/industries/financial-services/publications/insurance-2020-cyber.html. Accessed on June 5, 2024.
Shackelford, S.J., 2012. Should your firm invest in cyber risk insurance? Bus. Horiz. 55 (4), 349–356.
Shandler, R., Gomez, M.A., 2023. The hidden threat of cyber-attacks–undermining public confidence in government. J. Inf. Technol. Polit. 20 (4), 359–374.
Serra, A.P., 2004. Event study tests: a brief Survey. Gestão. Org-Revista Electrónica de Gestão Organizacional 2 (3), 248–255.
Sorescu, A., Warren, N.L., Ertekin, L., 2017. Event study methodology in the marketing literature: an overview. J. Acad. Mark. Sci. 45, 186–207.
Titman, S., Wessels, R., 1988. The determinants of capital structure choice. J. Finance 43 (1), 1–19.
Tosun, O.K., 2021. Cyber-Attacks and stock market activity. Int. Rev. Financ. Anal. 76, 101795.