The European Journal of Finance

ISSN: 1351-847X (Print) 1466-4364 (Online) Journal homepage: www.tandfonline.com/journals/rejf20

Analyzing spillover effects from data breaches to the US (cyber) insurance industry

Christian Eckert, Nadine Gatzert & Madeline Schubert

To cite this article: Christian Eckert, Nadine Gatzert & Madeline Schubert (2023) Analyzing spillover effects from data breaches to the US (cyber) insurance industry, The European Journal of Finance, 29:6, 669-692, DOI: 10.1080/1351847X.2022.2090267

To link to this article: https://doi.org/10.1080/1351847X.2022.2090267

THE EUROPEAN JOURNAL OF FINANCE
2023, VOL. 29, NO. 6, 669–692
https://doi.org/10.1080/1351847X.2022.2090267

Routledge
Taylor & Francis Group

Analyzing spillover effects from data breaches to the US (cyber) insurance industry

Christian Eckert[a], Nadine Gatzert [b] and Madeline Schubert[b]

[a]Department of Business and Economics, Coburg University of Applied Sciences and Arts, Coburg, Germany; [b]School of Business, Economics and Society, Friedrich-Alexander University Erlangen-Nürnberg (FAU), Nürnberg, Germany

ABSTRACT

As the US cyber insurance market is the largest worldwide, this paper presents an analysis of the effects of data breaches in the US financial services industry in relation to the stocks of US insurance companies. We conduct an event study, focusing on publicly announced data breaches that occurred between 2005 and 2018, and observe significant negative spillover effects for US insurers. However, in the subsample of non-announcing cyber insurers between 2015 and 2018, we not only find significant negative spillover effects especially for longer event windows, but also significant positive effects in case of 'mega data breaches' with more than 1 million breached records, which may be due to an increasing demand for cyber insurance. To understand these findings in more detail, we further analyze event as well as firm characteristics and find that spillover effects are information-based rather than pure.

ARTICLE HISTORY
Received 17 January 2022
Accepted 24 May 2022

KEYWORDS
Spillover effects; cyber loss events; cyber risk; data breach; event study

JEL CLASSIFICATIONS
G12; G14; G22; G32

1. Introduction

Firms exposed to cyberattacks, e.g. in the form of data breaches,[1] can suffer significant losses. A study by the Ponemon Institute (2019) finds that the global average cost of a data breach increased to USD 3.92 million in 2019, with 25,575 records as an average data breach size and a cost of USD 150 per lost record. However, cyberattacks might not only have a negative impact on the announcing firm's equity or debt. They could also spill over to third parties, e.g. competitors, insurers, investors or suppliers (see, e.g. Eckert, Gatzert, and Heidinger 2020, with respect to spillover effects from operational risk events in general). One explanation for spillover effects to insurance companies might be that they cover data breaches as a subset of cyberattacks and thus incur insured losses, and that the occurrence of cyberattacks provides new information regarding the loss frequency and severity of cyber risk. Moreover, insurance companies have a lot of sensitive data and might also be victims of future data breaches. To shed more light on this topic, the aim of our paper is to study spillover effects to the US insurance industry following data breaches on US financial services firms, a particularly sensitive issue given the data held by such companies. For this purpose, we focus on publicly announced data breaches between 2005 and 2018. We examine spillover effects from these events to non-announcing US insurance companies, based on stock market reactions, thereby also specifically examining a subsample of cyber insurers from 2015 to 2018. Finally, we analyze specific event and firm characteristics to explain the market implications of data breaches. This examination is also of high relevance as banks and insurers represent critical infrastructures, and cyber risk could become systemic (see World Economic Forum 2016).

Previous empirical literature regarding cyber risks has often focused on stock market implications (see, e.g. Malhotra and Kubowicz Malhotra 2011; Amir, Levi, and Livne 2018; McShane and Nguyen 2020; Kamiya et al. 2021) or reputational damage (see Sinanaj and Muntermann 2013; Kamiya et al. 2021) following data breaches

CONTACT Christian Eckert christian.eckert@hs-coburg.de

on the announcing firm. Thereby, different types of cyber risk incidents for publicly traded firms in the non-financial services industry or with(out) a specific industry focus have been examined as follows: data (security) breaches (see, e.g. Gatzlaff and McCullough 2010; Morse, Raval, and Wingender 2011); denial-of-service attacks (see Hovav and D'Arcy 2003); (information) security breaches (see, e.g. Campbell et al. 2003; Kannan, Rees, and Sridhar 2007; Goel and Shawky 2009; Gordon, Loeb, and Zhou 2011; Yayla and Hu 2011; Pirounias, Mermigas, and Patsakis 2014; Modi, Wiles, and Mishra 2015; Haislip et al. 2019); internet security breaches (see Cavusoglu, Mishra, and Raghunathan 2004); and virus announcements (see Hovav and D'Arcy 2005), while Eling and Wirfs (2019) have considered all types of cyber risk events. In addition to empirical findings, tangible and intangible costs for affected firms (see, e.g. Cavusoglu, Mishra, and Raghunathan 2004) or approaches to model and predict cyber hacking breaches (see, e.g. Xu et al. 2018) are discussed in the academic literature.

One strand of the literature on spillover effects (see, e.g. Eckert 2020, for an overview) focuses on operational risk events in general that result in spillover effects to non-announcing firms, as measured by means of market value losses (see, e.g. Cummins, Wei, and Xie 2012; Kaspereit et al. 2017; Eckert, Gatzert, and Heidinger 2020). Focusing on cyber incidents, spillover effects have been examined for e-security vendors (see Garg, Curtis, and Halper 2003), internet firms (see Ettredge and Richardson 2003), IT consulting firms (see Chen et al. 2012), retailers (see Kashmiri, Nicol, and Hsu 2017) or competitors in various industry sectors (see, e.g. Zafar, Ko, and Osei-Bryson 2012; Martin, Borah, and Palmatier 2017; Kamiya et al. 2021), most often based on event study methodology using buy-and-hold or cumulative abnormal returns. Baldwin et al. (2017) use a vector equation system to examine contagion in cybersecurity attacks, whereas Kelton and Pennington (2020) have investigated whether voluntary disclosure mitigates the cybersecurity breach contagion effect. Moreover, Corbet and Gurdgiev (2019) study spillover effects on financial markets by using the EGARCH model, while Caporale et al. (2021) analyze spillover effects in the cryptocurrency market using the VAR-GARCH process. Most closely related to our work is the research by Garg, Curtis, and Halper (2003) and Haislip et al. (2019), who study spillover effects not only to e-security vendors or competitors but also to insurance providers. Haislip et al. (2019) find significant negative spillover effects to cyber insurance providers and significantly different effects on insurers not offering cyber protection, but only with specific focus on cybersecurity breaches due to hacks. Moreover, Garg, Curtis, and Halper (2003) observe contagion effects for IT security breaches prior to 2002 and competitive effects for IT security breaches post 2002 for insurance carriers, without differentiating between insurers offering cyber insurance or not.

In this paper, we aim to extend the results of Garg, Curtis, and Halper (2003) and Haislip et al. (2019) in various ways. We explicitly focus on spillover effects to the insurance industry, and thereby expand the analysis in Eckert, Gatzert, and Heidinger (2020), who investigate spillover effects to the US and European insurance industry, based on operational risk events in general and without a focus on data breaches. In contrast to Garg, Curtis, and Halper (2003), who examine 22 selected IT security breaches between 1996 and 2002, and Haislip et al. (2019), who obtain cybersecurity breach data from Audit Analytics across 11 industries between January 2010 and March 2018, we base our study on various types of recorded data breaches in the financial services industry, using data from Privacy Rights Clearinghouse (PRC), the largest database with respect to publicly available data breaches between 2005 and 2018. This enables us to not only consider cybersecurity breaches due to 'hacks' as in the study by Haislip et al. (2019), but also all other types of breach. We then apply event study methodology, using the Fama-French (2015) five-factor model as the underlying estimation model for expected returns, to study the impact of data breaches on non-announcing US insurers. To gain further insight into the role of insurers covering data breaches, we further differentiate between the entire sample of 61 US insurers (for the complete observation period from 2005 to 2018) and a subsample of 14 identified cyber insurers, according to the National Association of Insurance Commissioners (NAIC) Cybersecurity and Identity Theft Coverage Supplement, from 2015 to 2018, as proposed by Eling and Zhu (2018) as well as Xie, Lee, and Eling (2020), who have studied cyber insurance offerings and performance of the US cyber insurance market. Moreover, we take into account various event and firm characteristics of non-announcing US insurers to better understand the drivers of the results.

In regard to spillover effects to all 61 non-announcing US insurers, we find significantly negative spillover effects (where contagion effects dominate competitive effects) following an announcement of a data breach in the financial services industry, based on cumulative abnormal returns (CARs). However, while the subsample of

14 non-announcing cyber insurers between 2015 and 2018 also exhibits significant negative effects, especially for longer event windows, we find that 'mega data breaches' with more than 1 million breached records can actually result in significant positive effects for non-announcing US cyber insurers, i.e. the competitive effect dominates the contagion effect, indicating that such data breaches might increase the sense of urgency regarding cyber protection, and might thus lead to increasing demand for cyber insurance. To explain spillover effects in more detail, we also investigate event characteristics, firm characteristics and similarities among announcing and non-announcing firms by means of regression analysis. We thereby find support for the hypothesis that the following produce significant spillover effects for US insurers: the number of breached records; the type of data breach; the return on assets (RoA); size; the capital opacity of the announcing firm; and the financial leverage of the non-announcing firm. Furthermore, we find evidence that the financial leverage of the announcing firm and the RoA of the non-announcing firm are significant influencing factors regarding spillover effects for US cyber insurers.

The remainder of the paper is organized as follows: Section 2 presents development of the hypotheses, and Section 3 describes our dataset and the methodology of our empirical analysis. Empirical results are presented in Section 4, and Section 5 concludes the paper.

$$\begin{aligned} R_{NA,j,t} - r_{f,t} = {} & \alpha_{NA,j} + \beta_{1_{NA,j}}(R_{m,t} - r_{f,t}) + \beta_{2_{NA,j}} SMB_t + \beta_{3_{NA,j}} HML_t + \beta_{4_{NA,j}} RMW_t \\ & + \beta_{5_{NA,j}} CMA_t + \varepsilon_{NA,j,t}, \end{aligned} \tag{1}$$

$$\begin{aligned} AR_{NA,j,t} = {} & R_{NA,j,t} - (\alpha_{NA,j} + \beta_{1_{NA,j}}(R_{m,t} - r_{f,t}) + \beta_{2_{NA,j}} SMB_t + \beta_{3_{NA,j}} HML_t \\ & + \beta_{4_{NA,j}} RMW_t + \beta_{5_{NA,j}} CMA_t + r_{f,t}). \end{aligned} \tag{2}$$

$$CAR_{NA,j}(\tau_1, \tau_2) = \sum_{t=\tau_1}^{\tau_2} AR_{NA,j,t} \tag{3}$$

$$\overline{CAR_{n;m;z}}(\tau_1, \tau_2) = \frac{1}{z} \cdot \sum_{j=1}^{n} \sum_{NA=1}^{m} CAR_{NA,j}(\tau_1, \tau_2) \tag{4}$$

$$\begin{aligned} CAR_{NA}(\tau_1, \tau_2) = {} & \alpha + \beta_1 BreachedRecords + \beta_2 RiskType + \beta_3 Size_A \\ & + \beta_4 RoA_A + \beta_5 Leverage_A + \beta_6 CapitalOpacity_A + \beta_7 Size_{NA} + \beta_8 RoA_{NA} \\ & + \beta_9 Leverage_{NA} + \beta_{10} RatioSize + \beta_{11} GeographicalDistance + \varepsilon_{NA}, \end{aligned} \tag{5}$$

2. Development of the hypotheses

To derive hypotheses regarding spillover effects from cyber risk incidents, competitive and contagion effects have to be distinguished as two offsetting effects, which result in spillover effects as the negative or positive net effect (see Lang and Stulz 1992; Eckert 2020). When a competitive effect occurs, non-announcing firms benefit from the announcement of the loss event, whereas a contagion effect implies a financial loss for non-announcing firms after the adverse event in the announcing firm (see Eckert 2020). In the following analysis, we report the net spillover effect, which implies that even if both individual effects are positive (and potentially large), they may offset each other and thus result in a net spillover effect of zero, which for us is the economically relevant figure (see also Barth et al. 2021).

Previous empirical research in the field of cyber risk has shown ambiguous findings and reveals both negative spillover effects (see, e.g. Hinz et al. 2015; Kashmiri, Nicol, and Hsu 2017; Kamiya et al. 2021, for competitor firms) and positive spillover effects (see, e.g. Cavusoglu, Mishra, and Raghunathan 2004, concerning internet security developers; Aytes, Byers, and Santhanakrishnan 2006, regarding non-confidential firm and customer information; Jeong, Lee, and Lim 2019, for competitors). An explanation for contagion effects in case of insurance companies is that such events convey new information regarding the loss frequency and severity of cyber risk events affecting insurers in two ways. First, insurers have a lot of sensitive data and might themselves be victims of future cyber risk events. Second, firms providing cyber insurance protection against attacks have to cover

such insured losses, and face a respective underwriting risk. However, due to a loss of trust in the announcing firm, customers might also substitute products and services of the announcing firm with products and services of non-announcing firms, if possible, leading to competitive effects. Moreover, data breaches could increase the risk awareness in companies, leading to an increasing demand for cyber insurance with resulting competitive effects for cyber insurers. In line with previous studies on announcing firms and spillover effects from data breaches (see Tables A1 and A2 in the Appendix for a review of the literature regarding cyber risk events and spillover effects, as well as Spanos and Angelis 2016, for instance), which are predominately measured by stock market reactions, we formulate our first Null hypothesis as follows:

Null hypothesis H_1: Data breaches do not result in spillover effects (in terms of cumulative abnormal stock returns) to non-announcing US (cyber) insurers.

Rejecting this Null hypothesis indicates that data breaches spill over from announcing to non-announcing US (cyber) insurers, which can result in a positive or negative net spillover effect, where the competitive effect dominates the contagion effect or vice versa. Otherwise, the competitive and contagion effect offset each other or are both non-existent.

To analyze spillover effects in more detail, we further investigate whether they are information-based or pure. Information-based spillover effects are thereby argued to result from rational repricing based on event and firm characteristics, which does not hold for pure spillover effects (see Aharony and Swary 1996; Cummins, Wei, and Xie 2012; Eckert, Gatzert, and Heidinger 2020). Hence, information-based spillover means that there are significant influencing factors on net spillover effects (competitive or contagion effects are affected). Cross-sectional analyses predominately indicate information-based spillover effects rather than pure effects (see, e.g. Aharony and Swary 1983; Cummins, Wei, and Xie 2012). We thus follow Eckert, Gatzert, and Heidinger (2020) and study hypotheses H_2–H_{12}, regarding specific event and firm characteristics of announcing US financial services firms and non-announcing US insurance companies serving as potential influencing factors for spillover effects for non-announcing US (cyber) insurers. Finding significant influencing factors indicates information-based spillover effects, while no significant influencing factors indicate pure spillover effects.

First, we focus on *event* characteristics that might influence spillover effects, starting with the number of breached records (*BreachedRecords*, H_2). On the one hand, data breaches in the financial services industry with a larger number of breached records may lead to stronger contagion effects for insurers in general, if these events convey new information to investors regarding a higher cyber loss severity, which may be transferred to non-announcing insurers as potential victims of such data breaches (see Kaspereit et al. 2017; Eckert, Gatzert, and Heidinger 2020). While this stronger contagion effect might similarly occur to non-announcing cyber insurers (see also Chen et al. (2012) for such an observation in case of IT consulting firms), they might also experience stronger competitive effects due to a higher risk awareness with a potentially resulting increase in cyber insurance demand. Hence, to investigate the effects of the number of breached records on the net effect (spillover effect) for US (cyber) insurers, we calculate the natural logarithm of the underlying total number of breached records and thus test.

Null hypothesis H_2: Spillover effects (in terms of cumulative abnormal stock returns) do not depend on the number of breached records.

We further distinguish the data breach risk type (*RiskType*, H_3) into 'malicious' risks with three subcategories and 'negligent' risks with four subcategories (see, e.g. Edwards, Hofmeyr, and Forrest 2016, and Section 3 for detailed explanations regarding event types).[2] On the one hand, malicious risk events could potentially lead to stronger contagion effects for non-announcing insurers than negligent risks events, since in particular these events might be interpreted as an indicator for an increasing likelihood of data breaches also for other companies. Negligent risk events, however, might rather reveal current firm-specific weaknesses of internal control systems that could be improved after occurrence of the damage. While this argumentation can analogously be transferred to cyber insurers, they might also exhibit stronger competitive effects particularly in case of malicious data breaches due to an expected increase in cyber insurance demand, which might be less likely for negligent risk, where the implementation of internal measures could already reduce the likelihood and severity of such events in non-announcing firms in the future or where coverage may not provided. To empirically investigate this issue

in more detail, we include data breach risk type as a dummy variable in our subsequent analysis, which is set to 1 for a malicious risk and 0 in the case of a negligent risk, and we test

Null hypothesis H_3: Spillover effects (in terms of cumulative abnormal stock returns) do not depend on the data breach risk type (malicious vs. negligent).

Besides event characteristics, we also aim to investigate *characteristics of the announcing firm*, which is why we further test Null hypotheses H_4–H_7. With respect to the size of the announcing firm (, H_4), measured by the natural logarithm of book value of total assets, we follow previous reasoning (see Akhigbe and Madura 2001; Kaspereit et al. 2017; Eckert, Gatzert, and Heidinger 2020) and assume that larger firms attract more attention and thus transfer more information to the capital markets (see Goins and Gruca 2008), potentially resulting in stronger spillover effects for (cyber) insurers due to new insight about the likelihood and severity of data breaches. Moreover, larger firms typically have more customers potentially leading to stronger competitive effects in case of customer churn from the announcing firm, which is why we test

Null hypothesis H_4: Spillover effects (in terms of cumulative abnormal stock returns) do not depend on the firm size of the announcing firm.

Fiordelisi, Soana, and Schwizer (2013) and Eckert, Gatzert, and Heidinger (2020) further argue that operational risk events in more profitable announcing firms are more surprising, might indicate a stronger reevaluation of the likelihood of such events in other firms and might, therefore, lead to stronger contagion effects. However, for cyber insurers, a higher risk awareness could also increase insurance demand, thus leading to stronger competitive effects. To study this relation in more detail, we measure profitability of the announcing firm using the return on assets (, H_5), and hypothesize

Null hypothesis H_5: Spillover effects (in terms of cumulative abnormal stock returns) do not depend on the Return on Assets of the announcing firm.

We further include the financial leverage of the announcing firm (, H_6) as a potential influencing factor to explain spillover effects to non-announcing (cyber) insurers, calculated by the book value of liabilities to market value of equity. According to Higgs et al. (2016), financially stronger equipped firms undertake more measures to counteract cyberattacks, which results in data breaches being more surprising with stronger contagion effects. Hence, we formulate

Null hypothesis H_6: Spillover effects (in terms of cumulative abnormal stock returns) do not depend on the financial leverage of the announcing firm.

Kamiya et al. (2021) show that firms with more intangible assets are more likely to suffer from a data breach. A data breach at such firms occurs, therefore, more often and is less surprising, which might lead to weaker contagion effects. At the same time, announcing firms with self-produced and valuable intangible assets (e.g. customer data, IT software) might also be more aware of the possibility of cybercrime, and therefore, be more engaged to protect their competitive advantage against data breaches. If despite this stronger protection a data breach occurs, this might indicate that the protection is less effective, leading to stronger contagion effects for firms in general, but potentially stronger competitive effects for cyber insurer. Moreover, firms with a higher capital opacity might have a more valuable customer base leading to stronger competitive effects if customers substitute products and services of the announcing firm with products and services of non-announcing firms. Thus, we include (H_7), measured by intangible assets to the book value of total assets, and test

Null hypothesis H_7: Spillover effects (in terms of cumulative abnormal stock returns) do not depend on capital opacity of announcing firm.

We additionally test hypotheses H_8–H_{10} to gain insights into the impact of *characteristics of non-announcing firms*. First, previous cyber risk literature has argued that especially large firms are a more attractive target for cybercriminals (see, e.g. Higgs et al. 2016) and have, in general, a greater likelihood of suffering a (future) data breach (see Higgs et al. 2016; Ettredge, Guo, and Yijun 2018; Kamiya et al. 2021). Therefore, data breaches revealing new information about the likelihood and severity are particularly relevant for such larger non-announcing

firms and might lead to stronger contagion effects on them. Thus, we include the size of the non-announcing (cyber) insurer (, H_8) and formulate:

Null hypothesis H_8: Spillover effects (in terms of cumulative abnormal stock returns) do not depend on the firm size of the non-announcing firmh.

We also include the profitability of the non-announcing firms (, H_9). Weaker contagion effects might arise from data breaches for more profitable non-announcing firms, as cost-effective companies have substantially more financial resources, enabling them to implement controls and reduce the likelihood of experiencing adverse events (see Kaspereit et al. 2017; Eckert, Gatzert, and Heidinger 2020). This reasoning is also supported by findings in Kamiya et al. (2021), who observe that well-performing peer firms are hurt less from data breaches on announcing firms. However, stronger contagion effects could also be the case, as profitable non-announcing firms might have specific cost reduction programs or saving strategies in place and, therefore, may not adequately invest in measures of cyber risk management or resilience. We thus hypothesize

Null hypothesis H_9: Spillover effects (in terms of abnormal stock returns) do not depend on the Return on Assets of the non-announcing firm.

As companies with more liabilities in terms of leverage (, H_{10}) are more likely to suffer financial distress and have a lower likelihood of regaining competitiveness after a similar cyber risk event as an announcing firm, such non-announcing firms might experience stronger contagion effects (see, e.g. Aharony and Swary 1996; Akhigbe and Madura 2001; Cummins, Wei, and Xie 2012; Eckert, Gatzert, and Heidinger 2020; as well as Garg 2020; and Kashmiri, Nicol, and Hsu 2017, for empirical evidence). However, Cummins, Wei, and Xie (2012) additionally argue that non-announcing firms with relatively low leverage are more likely to be targets of lawsuits, leading to an increasing likelihood of loss based on the 'deep pocket' theory of liability. The option-pricing theory also predicts that the stocks of less leveraged firms are more sensitive to new information, potentially implying stronger contagion effects (see Cummins, Wei, and Xie 2012). Overall, the financial distress theory thus supports the assumption that less leveraged firms will be less sensitive to (operational risk) events leading to weaker contagion effects, while deep-pocket and option-pricing theories implies the opposite. Hence, we test

Null hypothesis H_{10}: Spillover effects (in terms of cumulative abnormal stock returns) do not depend on the financial leverage of the non-announcing firm.

The final two hypotheses H_{11}–H_{12} refer to factors reflecting the similarity of investigated financial services firms and insurers, which might result in stronger market reactions (see Kaspereit et al. 2017; Eckert, Gatzert, and Heidinger 2020), as stakeholders might anticipate the occurrence of similar events (see, e.g. Yu, Sengul, and Lester 2008). To examine the similarities between companies, we first follow Eckert, Gatzert, and Heidinger (2020) and use (H_{11}), measured by one over the absolute difference between the natural logarithm of the size of the announcing financial services firms and non-announcing insurers. For a stronger size similarity, we anticipate stronger contagion effects as similar announcing and non-announcing firms might be penalized more and tend to be more susceptible to similar data breaches, which is consistent with empirical findings in Haislip et al. (2019) and Eckert, Gatzert, and Heidinger (2020). To investigate this in more detail, we hypothesize

Null hypothesis H_{11}: Spillover effects (in terms of cumulative abnormal stock returns) do not depend on the ratio of size between the announcing and non-announcing firm.

Moreover, firms that exhibit a stronger regional proximity (*GeographicalDistance*, H_{12}), measured as a dummy variable,[3] may experience similar economic conditions, which might lead to stronger spillover effects to firms in the same region (see also Aharony and Swary 1996; Brewer and Jackson 2002; Eckert, Gatzert, and Pisula 2019; Eckert, Gatzert, and Heidinger 2020; Barth et al. 2021). Non-announcing firms in the same region as the announcing firm might be more likely targeted, and therefore, suffer stronger contagion effects, and hypothesize

Null hypothesis H_{12}: Spillover effects (in terms of cumulative abnormal stock returns) do not depend on the geographical distance between the announcing and non-announcing firm.

3. Underlying event study methodology and data sample

3.1. Abnormal stock returns

We follow the approach in Eckert, Gatzert, and Heidinger (2020) and employ the Fama-French (2015) five-factor model as a benchmark model to measure stock market reactions for announcing firms and to assess spillover effects to non-announcing US insurance companies, given by

1) where the intercept is, factor loadings are, and the error term is, estimated by an ordinary least-squares (OLS) regression is the return of a non-announcing firm for the respective event *j* on day *t*. The five factors of Fama and French (2015) can be summarized as follows:[4] describes the excess return of the non-announcing insurer, reflects size (the daily return difference between small and large portfolios), and stands for high minus low (the daily return difference between high and low book-to-market-ratio portfolios). considers robust minus weak profitability (the daily return difference between respective portfolios), and describes conservative minus aggressive investment (the daily return difference between respective portfolios). Regarding the estimation period, we follow the approach in Kamiya et al. (2021) and use an estimation window of 220 trading days, where the estimation period is between 280 days and 61 days before announcement of the data breach. If the event day is a non-trading day, the next trading day is used as day 0. The daily abnormal stock return (*AR*) at the non-announcing firm *NA* is given by the difference between the observed and estimated return, i.e.

2) To obtain the cumulative abnormal stock return (*CAR*), the daily abnormal stock returns are summed up over the event window from day to day, i.e.

3) The mean CARs over *n* events, *m* non-announcing firms and *z* observations () are given by (see also Kamiya et al. 2021)

4) If the (mean) *CARs* have positive values, this means that competitive effects exceed the contagion effects, with negative net effects reflecting the opposite.

Based on the described event and firm characteristics in Section 2, we study the impact of 11 variables on spillover effects in order to test and to assess whether spillover effects are information-based or pure. If no significant variables are identified in the subsequent analysis, spillover effects are considered as pure rather than information-based. The multiple OLS regression model[5] can be described as (see, e.g. Eckert, Gatzert, and Heidinger 2020, for a similar approach)

5) where is the dependent variable of interest as the net spillover effect. In line with Kamiya et al. (2021), robust standard errors are adjusted for heteroscedasticity and also clustered at firm-level. We additionally include year-fixed effects, as done in Haislip et al. (2019), Garg (2020) and Kamiya et al. (2021).

3.2. Sample description

For the empirical study of spillover effects to the US insurance industry, we refer to publicly reported cyberattacks in the form of data breaches[6] from Privacy Rights Clearinghouse (PRC), which is the largest public database and widely used in academic cyber risk literature (see, e.g. Edwards, Hofmeyr, and Forrest 2016; Eling and Jung 2018; Xu et al. 2018; Leong and Chen 2020; Poyraz et al. 2020; Wheatley, Hofmann, and Sornette 2021). The database categorizes data breaches according to eight different types of breach[7] and eight types of business, and further provides additional information.[8] Eling and Jung (2018) emphasize that data reliability is given as information sources are provided and each event can easily be traced back. By continuously updating the database, PRC attempts to ensure the best possible data completeness (although this procedure also has its limitations[9]).

Our subsequent analysis is restricted to the business type 'Business Financial and Insurance Services', and we include all types of breaches (CARD, HACK, INSD, PHYS, PORT, STAT, DISC and UNKN). The preliminary sample consists of 786 data breaches between January 1st, 2005, and December 31st, 2018.[10] We exclude data breaches in the 'Unknown' category as no information regarding the type of event is available, which reduces the sample size to 713 data breaches. The extent of damage is quantified based on the number of breached records. The cases of zero breached records is excluded for three reasons: data are still undergoing examination; information regarding breached records are not made public, or the data breach has no effects (see Edwards, Hofmeyr, and Forrest 2016; Eling and Jung 2018). After exclusion of zero values, 362 data breaches remain in our sample. Moreover, we review our dataset once again with a focus on publicly listed companies suffering a

Table 1. Description of cyber losses in the 121 attacked financial services firms included in the sample (between 2005 and 2018).

Year	Loss frequency (Total number of data breaches, %)		Loss severity (Aggregated number of breached records, %)	
2005	6	4.96	5,547,623	1.10
2006	27	22.31	4,477,095	0.89
2007	18	14.88	15,253,973	3.02
2008	8	6.61	29,563,398	5.85
2009	3	2.48	135,000,120	26.70
2010	13	10.74	2,213,353	0.44
2011	15	12.40	552,773	0.10
2012	7	5.79	7,067,711	1.40
2013	4	3.31	793,419	0.16
2014	3	2.48	76,774,734	15.19
2015	5	4.13	80,382,324	15.90
2016	3	2.48	950,166	0.19
2017	2	1.65	145,512,000	28.78
2018	7	5.79	1,526,342	0.30
Total	121	100	505,615,031	100

data breach, which leads to 129 data breaches.[11] If more than one data breach has taken place on the same day, we remove these data breaches from our dataset as the potentially resulting spillover effects could not be disentangled (six cyber events). Similarly, we exclude data breaches involving more than one listed announcing financial services firm as we could not determine which announcing firm caused spillover effects to the non-announcing US (cyber) insurers. Thus, our final sample consists of 121 data breaches. Table 1 provides an overview of loss severity and frequency in the final sample, measured by the total number of data breaches and the aggregated number of breached records.

To empirically examine the spillover effects from data breaches to financial services firms (described in Table 1) to the US insurance industry between 2005 and 2018, we include US insurers with a recorded market capitalization available on December 31st, 2018 from Thomson Reuters Eikon. After removing insurance brokers, conglomerates and firms with other business models from the dataset, and including US insurers with available stock price data from 2005 to 2018, 61 US insurers remain in the sample.

Furthermore, a subsample of 14 insurers is identified that offered cyber insurance coverage from 2015 onwards, based on the Report on the Cybersecurity Insurance and Identity Theft Coverage Supplement from the NAIC (see Eling and Zhu 2018; Xie, Lee, and Eling 2020).[12] We observe that 18 out of the 121 data breaches considered from 2005 to 2018 occur to 9 US insurers in our sample, and the remainder concern firms outside of our sample. When studying spillover effects for these 18 data breaches, we consider the intra-industry implications for the remaining US insurers in our sample and remove observations for the announcing US insurers. The number of included observations is reduced when examining influencing factors in cases of limited data availability from Thompson Reuters Datastream.

4. Empirical results

4.1. Descriptive statistics

The summary statistics for all risk types based on our US financial services sample as well as the frequency of data breaches by risk type between 2005 and 2018 are provided in Table 2.

Table A3 in the Appendix additionally provides information regarding the top 10 cyber risk incidents based on the number of breached records in the financial services sample according to the PRC database. In addition, Table 3 shows summary statistics for event and firm characteristics of announcing and non-announcing US financial services firms and US (cyber) insurers.

Table 2. Summary of statistics and frequency of attack types in the sample of attacked financial services firms.

Risk type	Mean	Median	Std. Dev.	Min.	Max.	Number
I. Malicious risk	8,282,954	2000	28,637,715	11	145,500,000	58
CARD	781,261	950	2,332,044	100	7,000,000	9
HACK	13,103,069	5117	36,711,860	11	145,500,000	34
INSD	1,858,376	2000	4,717,832	12	17,000,000	15
II. Negligent risk	399,582	4100	1,668,433	1	12,500,000	63
DISC	41,601	1600	126,552	1	600,000	23
PHYS	1,675	1300	1,776	1	4,100	4
PORT	749,401	11,688	2,378,186	11	12,500,000	30
STAT	288,022	36,250	422,198	8	930,000	6

Notes: The summary statistics is based on the total number of breached records between 2005 and 2018. The frequency (number) of data breaches based on different breach types is shown in the last column.

Table 3. Summary statistics for event and firm characteristics of announcing and non-announcing US financial services firms/insurers.

	Mean	Std. Dev.	Min.	1st Quart.	Median	3rd Quart.	Max.
Panel A. Observations of announcing US financial services firms and non-announcing US insurers from 2005 to 2018 ($n = 6120$)							
Breached Records	8.9701	4.3131	0.0000	5.8522	8.5172	12.1118	18.7957
RiskType	0.4786	0.4996	0.0000	0.0000	0.0000	1.0000	1.0000
$Size_A$	17.8832	2.6077	12.9391	15.6496	18.3410	20.4355	21.6684
RoA_A	0.0103	0.0799	−0.7223	0.0062	0.0102	0.0224	0.1533
$Leverage_A$	8.8975	9.3929	0.0969	1.5083	6.4483	10.6380	49.1343
$CapitalOpacity_A$	0.1517	0.2367	0.0018	0.0146	0.0377	0.1684	0.8600
$Size_{NA}$	16.0038	2.1283	9.1507	14.8309	16.0980	17.1904	20.7820
RoA_{NA}	0.01836	0.0418	−0.5583	0.0065	0.0161	0.0344	0.2374
$Leverage_{NA}$	9.3671	51.2382	0.0522	1.8092	2.9944	6.5919	954.1981
RatioSize	1.3958	7.7248	0.0817	0.2155	0.3659	0.7607	308.5298
Geographical distance	0.0221	0.1469	0.0000	0.0000	0.0000	0.0000	1.0000
Panel B. Observations of announcing US financial services firms and non-announcing US **cyber** *insurers from 2015 to 2018 ($n = 224$)*							
Breached Records	8.6892	5.6403	0.0000	3.9160	8.2629	13.2650	18.7957
RiskType	0.5625	0.4972	0.0000	0.0000	1.0000	1.0000	1.0000
$Size_A$	17.1443	2.2028	13.1002	15.2991	17.2148	18.9629	20.6510
RoA_A	0.0176	0.0218	−0.0340	0.0086	0.0123	0.0251	0.0745
$Leverage_A$	6.9501	5.1431	0.2866	2.2133	6.1268	10.6380	18.7790
$CapitalOpacity_A$	0.1308	0.2018	0.0044	0.0096	0.0400	0.1523	0.7640
$Size_{NA}$	17.2829	1.3096	14.8222	16.4477	17.0268	18.4185	19.9982
RoA_{NA}	0.0133	0.0241	−0.1765	0.0046	0.0199	0.0248	0.0503
$Leverage_{NA}$	3.6560	3.1263	0.7044	1.8964	2.5581	3.8802	12.3793
RatioSize	1.8846	7.9537	0.1453	0.3209	0.5150	1.1233	107.3617
Geographical distance	0.0134	0.1152	0.0000	0.0000	0.0000	0.0000	1.0000

Notes: *BreachedRecords* is the natural logarithm of the number of total breached records from PRC. *RiskType* is coded as a dummy variable: 1 if the data breach is based on a malicious risk type (breach type categories CARD, HACK and INSD from PRC) and 0 if the data breach is based on a negligent risk type (breach type categories DISC, PHYS, PORT or STAT). $Size_A$ is the natural logarithm of the book value of total assets of the announcing firm from the US financial services industry. RoA_A is the return on assets, based on the annual net income-to-book value of total assets, and $Leverage_A$ is given by the book value of liabilities to market value of equity for the announcing firm. $CapitalOpacity_A$ is computed on the basis of the intangible assets-to-book value of total assets. $Size_{NA}$, RoA_{NA} and $Leverage_{NA}$ refers to the respective parameters for non-announcing US insurers. *RatioSize* is given by 1 over the absolute difference between $Size_A$ and $Size_{NA}$. *GeographicalDistance* is a dummy variable, set to 1 if the announcing firm is in the US state where the non-announcing US insurer's headquarter is located.

4.2. Empirical findings regarding spillover effects to US (cyber) insurers

The empirical results regarding spillover effects to US (cyber) insurers from data breaches on US financial services firms in our sample are presented in Table 4. We distinguish between spillover effects to all US insurers between 2005 and 2018 in Panel A, and to US *cyber* insurers between 2015 and 2018 in Panel B. The mean and median values of CARs are shown for different event windows after the announcement date. Two different significance tests are conducted following Kamiya et al. (2021).

Table 4. Empirical results for spillover effects in the US financial services industry to non-announcing US (cyber) insurance companies.

	Mean	*t*-statistic	*p*-value	Median	*z*-statistic	*p*-value
Panel A. Spillover effects from 121 data breaches in the US financial services industry to non-announcing US insurance firms between 2005 and 2018 (n = 7363)						
CAR (0, 0)	−0.0714%**	−2.5183	0.0118	−0.0418%***	−3.6180	0.0003
CAR (0, 1)	−0.0278%	−0.6929	0.4884	−0.0348%**	−1.7350	0.0827
CAR (0, 2)	−0.0920%*	−1.9076	0.0565	−0.0587%***	−2.7520	0.0059
CAR (0, 3)	−0.2655%***	−4.7076	0.0000	−0.1154%***	−4.7460	0.0000
CAR (0, 4)	−0.2432%***	−3.6622	0.0003	−0.1498%***	−5.4490	0.0000
CAR (0, 5)	−0.2711%***	−3.7725	0.0002	−0.2235%***	−5.2830	0.0000
CAR (−1, 1)	0.0368%	0.7649	0.4444	−0.0360%	−1.2300	0.2188
CAR (−2, 2)	−0.0896%	−1.4938	0.1353	−0.1300%***	−3.7170	0.0002
CAR (−3, 3)	−0.2835%***	−3.5669	0.0004	−0.2300%***	−5.7640	0.0000
CAR (−4, 4)	−0.2841%***	−3.0688	0.0022	−0.2788%***	−5.7570	0.0000
CAR (−5, 5)	−0.2489%**	−2.2543	0.0242	−0.2369%***	−4.4030	0.0000
Panel B. Spillover effects from 17 data breaches in the US financial services industry to non-announcing US cyber insurance firms between 2015 and 2018 (n = 238)						
CAR in %	Mean	*t*-statistic	*p*-value	Median	*z*-statistic	*p*-value
CAR (0, 0)	−0.1642%*	−1.8908	0.0599	−0.0580%*	−1.7710	0.0765
CAR (0, 1)	0.0077%	0.0657	0.9476	0.1163%	0.0570	0.9546
CAR (0, 2)	0.0287%	0.2169	0.8285	0.0318%	−0.4620	0.6439
CAR (0, 3)	0.0474%	0.3072	0.7589	−0.0593%	−0.8870	0.3749
CAR (0, 4)	−0.0080%	−0.0450	0.9642	−0.2003%	−1.1290	0.2589
CAR (0, 5)	0.1545%	0.7722	0.4408	−0.2293%	−0.5670	0.5710
CAR (−1, 1)	−0.0265%	−0.1786	0.8584	−0.0111%	−0.1860	0.8533
CAR (−2, 2)	−0.0968%	−0.5588	0.5768	−0.1987%	−1.6040	0.1087
CAR (−3, 3)	−0.1572%	−0.7796	0.4364	−0.4655%**	−2.5690	0.0102
CAR (−4, 4)	−0.3032%	−1.3238	0.1868	−0.6421%***	−3.0890	0.0020
CAR (−5, 5)	−0.2497%	−0.9043	0.3668	−0.6403%**	−2.3550	0.0185

Notes: *** denotes statistical significance at the 1% level, ** at the 5% level and * at the 10% level. As proposed by Kamiya et al. (2021), *t*-tests are used to evaluate the statistical significance for the mean CARs, and Wilcoxon signed-rank tests (non-parametric tests, z-statistic) are applied to assess the statistical significance for median CARs. In Panel B, we additionally observe a positive mean CAR (−1, 1) of 0.1430% at the 10% significance level when considering all data breaches from 2005 to 2018. Further robustness tests are shown in Table A4.

As shown in Table 4, Panels A and B, we observe significant net spillover effects and can, therefore, reject Null hypothesis H_1 for US insurers and US cyber insurers. With respect to which effect dominates, competitive versus contagion effect, for all announcing US insurers we find significantly negative spillover effects from data breaches in the US financial services industry (Panel A) for event windows (0, 0), (0, 2), (0, 3), (0, 4), (0, 5), (−3, 3), (−4, 4) and (−5, 5) regarding mean CARs, and for almost all event windows concerning median CARs, suggesting the dominance of contagion effects. Significant mean CARs range from −0.2841% to −0.0714%, and significant median CARs range from − 0.2788% to −0.0348%. The observed negative net effects are in line with the findings of Kamiya et al. (2021), who have also reported significant contagion effects to industry competitors based on data breaches (but without focusing on specific industries). Moreover, Eckert, Gatzert, and Heidinger (2020) also find more negative effects when studying spillover effects to US and European insurers based on operational risk events in general.

When considering the impact of data breaches on non-announcing US *cyber* insurers (Panel B), we find significant negative spillover effects for the mean CAR (0, 0) at the announcement day and for various median CARs in longer event windows (CAR (−3, 3), CAR (−4, 4) and CAR (−5, 5)), which is consistent with the results for insurers in general and may have been further negatively affected due to the related underwriting risk, as also reflected in more negative mean and median CARs. This generalizes the findings of Haislip et al. (2019), who observe a significant negative mean BHAR in the specific case of hacks for the event window (−5, 5), when examining spillover effects from various industries to US cyber insurers, and insignificant competitive effects for other event windows.

Moreover, in Table 5 we study the effect of the intensity of data breaches on the basis of the number of breached records for four intervals (more than 1000/10,000/100,000/1 million breached records). For the first three intervals, we also find significant negative spillover effects to US cyber insurers. However, in the case of 'mega data breaches' with more than 1 million breached records, we exclusively observe strong positive spillover effects to US cyber insurers for event windows (0, 1), (0, 2), (−1, 1) and (−2, 2), with mean CARs ranging from 0.2885% to 0.7187% and median CARs ranging from 0.1737% to 0.7175%. These results provide a first indication that 'mega data breaches' may trigger an increased sense of urgency regarding cyber protection with an increasing demand for cyber insurance, and therefore, dominating competitive effects.

To study relevant event and firm characteristics in more detail and to identify information-based versus pure spillover effects, we apply regression analyses. As we observe the highest significance level for mean/median CARs for all non-announcing US insurers in the event window (0, 5) (see Table 4, Panel A) and for non-announcing US cyber insurers in the event window (−4, 4) (see Table 4, Panel B), we use the mean CAR (0, 5) and CAR (−4, 4) as the dependent variables of interest in the base case of the regression analyses, as is similarly done in Eckert, Gatzert, and Heidinger (2020). Additionally, we vary the underlying event windows to investigate the robustness of the results. The results are shown in Table 6. The reported R2 is low when studying all non-announcing US insurers (see Table 6, Panel A), which is similar to other spillover studies concerning operational risk events (see Cummins, Wei, and Xie 2012; Kaspereit et al. 2017; Eckert, Gatzert, and Heidinger 2020) and cybersecurity breaches (see Haislip et al. 2019).

Panel A of Table 6 reveals six significant variables. *BreachedRecords*, *RiskType*, RoA_A *and* $Leverage_{NA}$ have a significant negative impact on spillover CARs, while $Size_A$ and $CapitalOpacity_A$ have a significant positive effect. This indicates that a data breach with a high number of breached records and data breaches of a malicious risk type led to dominating contagion effects for non-announcing US insurers during the period studied. Moreover, data breaches to more profitable announcing firms also implied adverse effects for non-announcing US insurers due to a stronger reevaluation of the likelihood of data breaches in the insurance industry. Highly leveraged non-announcing US insurers also suffer more from spillover effects, indicating support for the financial distress theory, i.e. higher leveraged companies are more vulnerable to financial distress. Hence, a higher likelihood of data breaches as indicated by the event in the announcing firm is more relevant for them, leading to stronger contagion effects. On the other hand, size and capital opacity of announcing firms positively impact the CARs of non-announcing US insurers. This might be the case as large announcing financial services firms have a large customer base and, therefore, a larger number of customers who can switch to non-announcing companies, implying stronger competitive effects. Furthermore, firms with valuable, self-produced intangible assets are more likely to suffer from a data breach, and events at such companies are less surprising, leading to weaker contagion effects.

In Table 6, Panel B, it can also be seen that the level to which US cyber insurers profit depends on the leverage of announcing firms, which might increase demand for cyber insurance and lead to positive effects, whereas RoA_{NA} causes negative effects, with one explanation being that more profitable non-announcing firms might have cost reduction strategies in place, which hamper the resilience of the firm against data breaches.

Overall, we can reject the six corresponding Null hypotheses regarding *BreachedRecords* (H_2), *RiskType* (H_3), $Size_A$ (H_4), RoA_A (H_5), $CapitalOpacity_A$ (H_7) and $Leverage_{NA}$(H_{10}) for all non-announcing US insurers, and the two Null hypothesis regarding $Leverage_A$(H_6) and RoA_{NA} (H_9) for US cyber insurers. This also leads us to conclude that spillover effects from data breaches are information-based rather than pure, which is in line with the findings of Cummins, Wei, and Xie (2012), Haislip et al. (2019), Eckert, Gatzert, and Heidinger (2020) and Kamiya et al. (2021).

When conducting regression analyses again for all 11 event windows for all non-announcing US insurers (see Tables 4 and 6, Panel A), *BreachedRecords*, *RiskType*, $Size_A$, RoA_A, $CapitalOpacity_A$ *and* $Leverage_{NA}$ have a significant effect in 4, 3, 10, 9, 10 and 7 cases (out of 11), respectively. For non-announcing US cyber insurers, the variable $Leverage_A$ *and* RoA_{NA} is significant in 10 and 9 cases, respectively (see Table 6, Panel B).

Furthermore, we vary the factors influencing spillover effects for our base case (CAR (0, 5) and CAR (−4, 4)) for all non-announcing US insurers and cyber insurers. With respect to H_3 we previously differentiate between a malicious risk (data breach type *CARD, HACK* and *INSD* from PRC) and a negligent risk (data breach type *DISC, PHYS, PORT* and *STAT* from PRC) in Table 6. We now run the regression for our base case (CAR (0, 5)

Table 5. Empirical results for spillover effects in the US financial services industry to non-announcing US cyber insurance companies depending on the number of breached records.

	Mean	*t*-statistic	*p*-value	Median	*z*-statistic	*p*-value
*Panel A. Spillover effects from 9 out of 17 data breaches (***with more than 1,000 breached records***) in the US financial services industry to non-announcing US cyber insurance firms between 2015 and 2018 (n = 126)*						
CAR (0, 0)	−0.3793%***	−2.9470	0.0038	−0.1792%***	−2.8280	0.0047
CAR (0, 1)	−0.1523%	−0.9663	0.3357	0.0472%	−0.4320	0.6656
CAR (0, 2)	−0.0783%	−0.4428	0.6587	−0.0650%	−0.7490	0.4540
CAR (0, 3)	−0.0996%	−0.4856	0.6281	−0.1865%	−1.3990	0.1619
CAR (0, 4)	−0.0965%	−0.4478	0.6550	−0.2003%	−1.2230	0.2212
CAR (0, 5)	0.2200%	0.8526	0.3955	−0.0977%	−0.0770	0.9400
CAR (−1, 1)	−0.3136%	−1.5855	0.1154	−0.1212%	−0.9290	0.3530
CAR (−2, 2)	−0.4505%**	−2.0809	0.0395	−0.3381%**	−2.3290	0.0199
CAR (−3, 3)	−0.6766%***	−2.7783	0.0063	−0.8748%***	−3.8480	0.0001
CAR (−4, 4)	−0.7672%**	−2.5870	0.0108	−1.0219%***	−3.8190	0.0001
CAR (−5, 5)	−0.5781%	−1.5218	0.1306	−1.1571%***	−2.6890	0.0069
*Panel B. Spillover effects from 8 out of 17 data breaches (***with more than 10,000 breached records***) in the US financial services industry to non-announcing US cyber insurance firms between 2015 and 2018 (n = 112)*						
CAR (0, 0)	−0.4734%***	−3.4635	0.0008	−0.3518%***	−3.5040	0.0005
CAR (0, 1)	−0.1655%	−1.0171	0.3113	0.0744%	−0.3600	0.7189
CAR (0, 2)	−0.1460%	−0.8086	0.4205	−0.0839%	−0.9990	0.3180
CAR (0, 3)	−0.1912%	−1.0593	0.2918	−0.1865%	−1.4860	0.1372
CAR (0, 4)	−0.1681%	−0.8103	0.4195	−0.2330%	−1.2690	0.2046
CAR (0, 5)	0.1042%	0.4371	0.6629	−0.0977%	−0.1250	0.9007
CAR (−1, 1)	−0.2897%	−1.3951	0.1658	0.0087%	−0.2610	0.7939
CAR (−2, 2)	−0.5669%**	−2.5484	0.0121	−0.3784%**	−2.4420	0.0146
CAR (−3, 3)	−0.6754%***	−2.9881	0.0035	−0.7705%***	−3.3970	0.0007
CAR (−4, 4)	−0.7743%***	−2.6899	0.0083	−1.0219%***	−3.5450	0.0004
CAR (−5, 5)	−0.6512%*	−1.7762	0.0784	−0.9357%**	−2.4040	0.0162
*Panel C. Spillover effects from 5 out of 17 data breaches (***with more than 100,000 breached records***) in the US financial services industry to non-announcing US cyber insurance firms between 2015 and 2018 (n = 70)*						
CAR (0, 0)	−0.4006%**	−2.0446	0.0447	−0.2455%**	−1.9810	0.0476
CAR (0, 1)	−0.0069%	−0.0313	0.9751	0.1262%	0.5300	0.5964
CAR (0, 2)	0.2803%	1.1503	0.2540	0.1267%	1.1560	0.2478
CAR (0, 3)	0.1983%	0.8470	0.3999	0.1743%	0.6350	0.5255
CAR (0, 4)	0.1285%	0.4615	0.6459	−0.0911%	0.0730	0.9417
CAR (0, 5)	0.0744%	0.2546	0.7998	−0.2247%	−0.2600	0.7945
CAR (−1, 1)	0.0459%	0.1742	0.8622	0.3964%	1.5070	0.1318
CAR (−2, 2)	−0.0809%	−0.2766	0.7829	0.1044%	0.1320	0.8952
CAR (−3, 3)	−0.1948%	−0.7103	0.4799	−0.3264%	−0.6930	0.4880
CAR (−4, 4)	−0.2601%	−0.7385	0.4627	0.1044%	−1.0860	0.2777
CAR (−5, 5)	−0.5776%	−1.2871	0.2023	−0.3279%	−1.2080	0.2269
*Panel D. Spillover effects from 3 out of 17 data breaches (***with more than 1,000,000 breached records***) in the US financial services industry to non-announcing US cyber insurance firms between 2015 and 2018 (n = 42)*						
CAR (0, 0)	−0.3321%	−1.3289	0.1912	−0.0063%	−1.0940	0.2739
CAR (0, 1)	0.2885%*	1.6987	0.0970	0.1737%*	1.6570	0.0976
CAR (0, 2)	0.7184%**	2.5052	0.0163	0.3492%**	2.0820	0.0374
CAR (0, 3)	0.3059%	0.9544	0.3455	0.1426%	0.5810	0.5610
CAR (0, 4)	0.1282%	0.3225	0.7487	−0.2288%	−0.2440	0.8074
CAR (0, 5)	0.0923%	0.2245	0.8234	−0.4064%	−0.1940	0.8463
CAR (−1, 1)	0.7187%***	3.7822	0.0005	0.7175%***	3.3320	0.0009
CAR (−2, 2)	0.7102%**	2.3930	0.0214	0.5061%*	1.8940	0.0582
CAR (−3, 3)	0.2923%	0.9625	0.3414	−0.4309%	0.3690	0.7122
CAR (−4, 4)	0.1155%	0.2743	0.7853	−0.1967%	−0.1060	0.9154
CAR (−5, 5)	−0.3730%	−0.5819	0.5638	−0.3458%	−0.4810	0.6302

Notes: *** denotes statistical significance at the 1% level, ** at the 5% level and * at the 10% level. As proposed by Kamiya et al. (2021), *t*-tests are used to evaluate the statistical significance for the mean CARs, and Wilcoxon signed-rank tests (non-parametric tests, *z*-statistic) are applied to assess the statistical significance for median CARs. Further robustness tests are shown in Table A5.

and CAR (−4, 4)) for all non-announcing US insurers and cyber insurers by including three dummy variables[13] for the malicious data breach type. Thereby, we find a significant positive impact of $Size_A$ (0.00084***) and $CapitalOpacity_A$ (0.01023**) on spillover CARs and a negative one for *BreachedRecords* (−0.00055***), *INSD*

Table 6. Analysis of factors influencing spillover effects for non-announcing US insurers (dependent variable is CAR (0, 5) in Panel A and CAR (−4, 4) in Panel B).

	Panel A All non-announcing US insurers between 2005 and 2018 (n = 6,120)			Panel B Non-announcing US cyber insurers between 2015 and 2018 (*n* = 224)		
	Regression coefficients	*t*-statistic	*p*-value	Regression coefficients	*t*-statistic	*p*-value
Breached Records	−0.00056***	−3.5692	0.0007	0.00035	0.3007	0.7684
RiskType	−0.00359**	−2.2609	0.0274	−0.00061	−0.1105	0.9137
$Size_A$	0.00081**	2.3385	0.0227	0.00144	0.9952	0.3378
RoA_A	−0.07114***	−3.3578	0.0014	−0.11191	−0.6295	0.5399
$Leverage_A$	0.00008	0.7060	0.4829	0.00124***	3.7936	0.0022
$CapitalOpacity_A$	0.01008**	2.4130	0.0189	0.00453	0.2379	0.8156
$Size_{NA}$	0.00041	0.8866	0.3788	−0.00540	−1.7654	0.1010
RoA_{NA}	0.09397	1.6110	0.1124	−0.26474*	−1.9599	0.0718
$Leverage_{NA}$	−0.00005***	−5.2299	0.0000	0.00160	0.9102	0.3793
RatioSize	0.00003	0.7721	0.4431	−0.00001	−0.0724	0.9434
Geographical Distance	−0.00969	−1.6440	0.1054	−0.02953	−1.2477	0.2341
Intercept	−0.01986*	−2.04397	0.0454	0.05300	1.3950	0.1864
R^2	0.0209			0.1308		
P-value F	0.0000			0.0000		

Notes: *** denotes statistical significance at the 1% level, ** at the 5% level and * at the 10% level. The dependent variable is CAR (0, 5) in Panel A and CAR (−4, 4) in Panel B. When using the event window (−4, 4) as dependent variable for the regression in Panel A, *RiskType* becomes insignificant. Breached records are the natural logarithm of the number of total breached records from PRC. *RiskType* is coded as a dummy variable: 1 if the data breach is based on a malicious risk type (breach type categories CARD, HACK and INSD from PRC) and 0 if the data breach is based on a negligent risk type (breach type categories DISC, PHYS, PORT or STAT). $Size_A$ is the natural logarithm of the book value of total assets of the announcing firm in the US financial services industry. RoA_A is the return on assets, based on the annual net income-to-book value of total assets; and $Leverage_A$ is the book value of liabilities to the market value of equity in the announcing firm. $CapitalOpacity_A$ is computed on the basis of intangible assets to the book value of total assets. $Size_{NA}$, RoA_{NA} and $Leverage_{NA}$ refer to the respective parameters for non-announcing US insurers. *RatioSize* is given by 1 over the absolute difference between $Size_A$ and $Size_{NA}$. *GeographicalDistance* is a dummy variable: set to 1 if the announcing firm was in the US state where the non-announcing US insurer's headquarter is located. Robust standard errors are clustered at the firm-level of non-announcing US insurers. The inclusion of year-fixed effects led to an increasing R^2 (0.0370 and 0.1801) for both regression models (Panels A and B), but also increasing VIFs and are, therefore, not included. When clustering robust standard errors based on events, following Kaspereit et al. (2017) and Eckert, Gatzert, and Heidinger (2020), RoA_A, RoA_{NA} and *GeographicalDistance* are found to be statistically significant (see Panel A), and $Size_{NA}$ is found to be significant (Panel B.). We additionally run the regression with adjusted robust standard errors for heteroscedasticity. In this case, $Leverage_{NA}$ (Panel A.) becomes insignificant, whereas all other variables are still significant, and *GeographicalDistance* additionally becomes significant. As can be seen from Panel B, $Size_{NA}$ becomes significant, but the *p*-value *F* is 0.3313. Further robustness tests are shown in Table A6.

(−0.00567***), RoA_A (−0.07160***) and $Leverage_{NA}$ (− 0.00005***). We also observe a significant negative effect of the data breach type RoA_{NA} (- 0.26512*) and a significant positive effect of $Leverage_A$ (0.00123***) on spillover CARs for non-announcing US cyber insurers.

Finally, as reported in the notes of Tables 4–6, we conducted further robustness checks by additionally excluding data breaches during event windows that also included confounding events such as earnings announcement or multiple data breach events, which resulted in stable outcomes for almost all event windows except for at most one (only weakly significant) exception per Panel, respectively.

5. Conclusion

This paper contributes to the literature by studying spillover effects from data breaches occurring to US financial services firms to non-announcing US (cyber) insurance companies, based on an event study methodology. The empirical analysis comprises 121 data breaches in US financial services firms (according to data from Privacy Rights Clearinghouse, the largest public database on data breaches in the US). In contrast to previous literature, we specifically concentrate on the financial services industry and include all types of attacks. We study spillover effects to 61 non-announcing US insurers between 2005 and 2018 using a Fama-French (2015) five-factor model, and additionally examine spillover effects to 14 US cyber insurers in our sample between 2015 and 2018. We also study potential factors influencing the sign and strength of spillover effects to the non-announcing US (cyber) insurance industry by applying regression analyses.

The results show significant cumulative abnormal returns (CARs), confirming the hypothesis of significant spillover effects to non-announcing US insurers following announcement of a data breach in the US financial services industry. In particular, we observe significant negative spillover effects for all non-announcing US insurers in the sample between 2005 and 2018, as well as significant positive spillover effects for non-announcing US *cyber* insurers between 2015 and 2018 when focusing on 'mega data breaches' with more than 1 million breached records, as their occurrence may lead to increasing demand for cyber insurance. Besides positive spillover effects, where the competitive effect exceeds the contagion effect, we also observe significant negative spillovers for US cyber insurers when we do not distinguish in regard to the number of breached records, especially for a longer event window, which may be due to underwriting risk.

When analyzing influencing factors relating to spillover effects by means of regression analyses, we find significant results for event and firm characteristics. With respect to the similarity between firms, our results are only significant in the case of 'mega data breaches', which also implies that the observed spillover effects are information-based rather than pure. For all US insurers, we find that a high number of breached records, malicious data breaches as well as data breaches on profitable financial services firms cause negative spillover effects for non-announcing insurers. Highly leveraged non-announcing insurers also experience negative effects, whereas the size and capital opacity of announcing financial services firms positively influence the CARs of non-announcing insurers.

With respect to practical implications, the fact that we predominantly observe contagion effects illustrates a high degree of uncertainty in regard to loss frequency and loss severity of data breaches in the market as well as potential challenges of cyber risk management (assessment and mitigation) of (non-announcing) firms perceived in the market. Therefore, from a managerial perspective appropriate (cyber and) spillover risk management measures are essential to encounter data breaches and their impact for both announcing and non-announcing firms. Regarding future research, a possible extension of our analysis would be to also take into account the cyber insurance gap, i.e. the share of the cyber losses that are covered by insurance, and to investigate its impact on spillover effects.

For cyber insurers in particular, managerial implications are mixed. On the one hand, the demand for cyber insurance might increase, especially after 'mega data breaches' due to a higher awareness regarding cyber risks, which can represent a business opportunity. On the other hand, however, there appears to be considerable underwriting risk for cyber insurers. Especially against the background of the rapidly changing nature of cyber risks and the digital transformation with an increasing amount of data, insurers are advised to reconsider their cyber insurance product components and its profitability on an ongoing basis.

Notes

1. Privacy Rights Clearinghouse (2018) provides an overview of different definitions of 'data breach', based on US state breach notification laws (https://privacyrights.org. Accessed January 4, 2022: 'A data breach is a security violation in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an unauthorized individual. It could be a result of hacking, theft of credit/debit card numbers, lost, discarded or stolen documents/devices, mishandled sensitive information'). Note that the term 'cyberattack' is typically understood as broader according to Eling, McShane, and Nguyen (2021) and may also refer to events such as phishing, cyber extortions or denial of service attacks.
2. Another categorization approach is used in Poyraz et al. (2020) to examine two specific data breach types more closely (data breaches involving personally identifiable information (PII) and sensitive personally identifiable information (SPII) data breaches), leading to a sample size of 134 incidents, out of more than 9,000 recorded data breaches across all industries, and a final sample set of 30, which, given the small sample size, is outlined as a limitation of their research. Wheatley, Hofmann, and Sornette (2021) have used the HACK, DISC, INSD and NA subcategories of the PRC database and introduced HW as a category for all physical assets, when addressing insurance of data breach cyber risk in the catastrophe framework.
3. We identify the state of announcing firms based on the geographic coordinates from Privacy Rights Clearinghouse. Regarding non-announcing firms, we refer to the headquarters or jurisdiction of the incorporation provided in SEC 10-K reports. In the case of unavailable SEC 10-K reports, we conduct an internet search to identify the US state of firms' headquarters. The dummy variable is set to 1 if the announcing and non-announcing firms are located in the same US state, and 0 otherwise.
4. We would like to thank Kenneth French for providing these factors for the five-factor model for US insurers, at https://mba.tuck.dartmouth.edu/pages/faculty/ken.french/data_library.html.

5. Multicollinearity does not pose a problem in our empirical examination as the absolute correlation coefficients are below a threshold value of 0.8 (see Mason and Perreault 1991), and the variance inflation factors (VIFs) are also below the threshold of 10 (see Marquardt 1970).
6. All 50 US states have introduced legislation that requires enterprises to report breaches of information to the individuals concerned (the first state to do this being California in 2002) (see PRC 2018; National Conference of State Legislatures (NCSL) 2020). In this context, PRC (2018) provides a comprehensive overview of US state data-breach notification statutes, along with definitions of data breaches at state level. Note that the PRC database restricts the scope of this study in the sense that PRC contains only records of data breaches, whereas the term 'cyberattack' is commonly recognized as a superset of that, including not only data breaches, but also other events, e.g., phishing, cyber extortion or denial of service attacks (see the literature review by Eling, McShane, and Nguyen 2021), which are not recorded in the PRC database. Empirical papers that are based on the same database include Eling and Jung (2018), Xu et al. (2018), and Wheatley, Hofmann, and Sornette (2021).
7. The different types of breaches are**: CARD =** 'Fraud Involving Debit and Credit Cards Not Via Hacking (skimming devices at point-of-service terminals, etc.)'; HACK = 'Hacked by an Outside Party or Infected by Malware'; **INSD** = 'Insider (employee, contractor or customer)'; **PHYS** = 'Physical (paper documents that are lost, discarded or stolen)'; **PORT** = 'Portable Device (lost, discarded or stolen laptop, PDA, smartphone, memory stick, CDs, hard drive, data tape, etc.)'; **STAT** = 'Stationary Computer Loss (lost, inappropriately accessed, discarded or stolen computer or server not designed for mobility)'; **DISC** = 'Unintended Disclosure Not Involving Hacking, Intentional Breach or Physical Loss (sensitive information posted publicly, mishandled or sent to the wrong party via publishing online, sending in an email, sending in a mailing or sending via fax)'; **UNKN** = 'Unknown (not enough information about breach to know how exactly the information was exposed)' (see https://privacyrights.org/data-breaches, accessed: 05/16/2020).
8. This information includes a breach date made public, the company, event location (city, state, geographic coordinates), total number of breached records, description of incidents, information source and year of breach.
9. For instance, the database only contains publicly published cyber losses, and there is the possibility of backfilling bias (see Edwards, Hofmeyr, and Forrest 2016; Eling and Jung 2018).
10. The data were extracted from PRC (see https://privacyrights.org/data-breaches, accessed: 04/19/2020 and checked once again on 09/10/2021).
11. We thereby include listed parent companies of related unlisted subsidiaries (see also Kamiya et al. 2021), and we exclude listed financial services firms and parent companies headquartered outside the US or those which became listed after the data breach. Furthermore, we exclude data breaches listed more than once, and in case of listed non-financial firms, e.g., when two or more firms were involved in one data breach, where one unlisted firm belongs to the financial services industry, and the other listed firms belong to the non-financial industry sector.
12. The NAIC provides two reports on the Cybersecurity and Insurance and Identity Theft Coverage Supplement in 2019 and 2020, which comprise the top 20 groups writing stand-alone cyber insurance, as well as the top 20 groups writing package policies for cyber insurance by direct written premiums in 2018 and 2019 (see also https://www.naic.org, accessed: 03/21/2021).
13. When solely including 'HACK' as a dummy variable, we observe a significant positive impact of $Size_A$ (0.00072***) and $CapitalOpacity_A$ (0.00996**) on spillover CARs and a negative one for *BreachedRecords* (- 0.00056***), RoA_A (-0.07166***) and $Leverage_{NA}$ (-0.00005***) for the sample containing all insurers. Moreover, we find a positive effect of $Leverage_A$ (0.00123***) on spillover CAR for cyber insurers and a negative one for RoA_{NA} (-0.26515*).

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

This work was supported by the School of Business, Economics and Society of the Friedrich-Alexander-Universität Erlangen-Nürnberg.

Notes on contributor

After working as a research assistant at Friedrich-Alexander University Erlangen-Nürnberg, ***Madeline Schubert*** is now risk manager at HUK-Coburg.

ORCID

Nadine Gatzert http://orcid.org/0000-0001-8321-1556

References

Aharony, J., and I. Swary. 1983. "Contagion Effects of Bank Failures: Evidence from Capital Markets." *Journal of Business* 56 (3): 305–322.

Aharony, J., and I. Swary. 1996. "Additional Evidence on the Information-Based Contagion Effects of Bank Failures." *Journal of Banking & Finance* 20 (1): 57–69.

Akhigbe, A., and J. Madura. 2001. "Why do Contagion Effects Vary Among Bank Failures?" *Journal of Banking & Finance* 25 (4): 657–680.

Amir, E., S. Levi, and T. Livne. 2018. "Do Firms Underreport Information on Cyber-Attacks?" *Evidence From Capital Markets. Review of Accounting Studies* 23: 1177–1206.

Aytes, K., S. Byers, and M. Santhanakrishnan. 2006. "The Economic Impact of Information Security Breaches: Firm Value and Intra-Industry Effects." *American Conference on Information Systems (AMCIS) 2006 Proceedings*, 399.

Baldwin, A., I. Gheyas, C. Ioannidis, D. Pym, and J. Williams. 2017. "Contagion in Cyber Security Attacks." *Journal of the Operational Research Society* 68: 780–791.

Barth, F., C. Eckert, N. Gatzert, and H. Scholz. 2021. "An Empirical Analysis of Spillover Effects from the Volkswagen Emission Scandal: An Analysis of Stock and Corporate Bond Markets." *Schmalenbach Journal of Business Research* 74 (1): 37–76.

Brewer, E., and W. E. Jackson. 2002. *Inter-Industry Contagion and the Competitive Effects of Financial Distress Announcements: Evidence from Commercial Banks and Life Insurance Companies*. Working Paper. Federal Reserve Bank of Chicago.

Campbell, K., L. A. Gordon, M. P. Loeb, and L. Zhou. 2003. ": The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market." *Journal of Computer Security* 11 (2003): 431–448.

Caporale, G. M., W.-Y. Kang, F. Spagnolo, and N. Spagnolo. 2021. "Cyber Attacks, Spillovers and Contagion in the Cryptocurrency Markets." *Journal of International Financial Markets, Institutions & Money* 74: 101298.

Cavusoglu, H., B. Mishra, and S. Raghunathan. 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 (1): 69–104.

Chen, J. V., H.-C. Li, D. C. Yen, and K. V. Bata. 2012. "Did IT Consulting Firms Gain When Their Clients Were Breached?" *Computers in Human Behavior* 28: 456–464.

Corbet, S., and C. Gurdgiev. 2019. ": What the Hack: Systematic Risk Contagion from Cyber Events." *International Review of Financial Analysis* 65: 101386.

Cummins, J. D., R. Wei, and X. Xie. 2012. *Financial Sector Integration and Information Spillovers: Effects of Operational Risk Events on U.S. Banks and Insurers*. Working Paper. California State University.

Eckert, C. 2020. "Risk and Risk Management of Spillover Effects: Evidence from the Literature." *Risk Management and Insurance Review* 23 (1): 75–104.

Eckert, C., N. Gatzert, and D. Heidinger. 2020. ": Empirically Assessing and Modeling Spillover Effects from Operational Risk Events in the Insurance Industry." *Insurance: Mathematics and Economics* 93: 72–83.

Eckert, C., N. Gatzert, and A. Pisula. 2019. ": Spillover Effects in the European Financial Services Industry from Internal Fraud Events: Comparing Three Cases of Rogue Trader Scandals." *Journal of Risk Finance* 20 (3): 249–266.

Edwards, B., S. Hofmeyr, and S. Forrest. 2016. ": Hype and Heavy Tails: A Closer Look at Data Breaches." *Journal of Cybersecurity* 2 (1): 3–14.

Eling, M., and K. Jung. 2018. ": Copula Approaches for Modeling Cross-Sectional Dependence of Breach Losses." *Insurance: Mathematics and Economics* 82: 167–180.

Eling, M., M. McShane, and T. Nguyen. 2021. ": Cyber Risk Management: History and Future Research Directions." *Risk Management and Insurance Review* 24 (1): 1–33.

Eling, M., and J. H. Wirfs. 2019. "What are the Actual Costs of Cyber Risk Events?" *European Journal of Operational Research* 272 (3): 1109–1119.

Eling, M., and J. Zhu. 2018. "Which Insurers Write Cyber Insurance? Evidence from the U.S. Property and Casualty Insurance Industry." *Journal of Insurance Issues* 41 (1): 22–56.

Ettredge, M. L., F. Guo, and L. Yijun. 2018. "Trade Secrets and Cyber Security Breaches." *Journal of Accounting and Public Policy* 37: 564–585.

Ettredge, M. L., and V. J. Richardson. 2003. ": Information Transfer Among Internet Firms: The Case of Hacker Attacks." *Journal of Information Systems* 17 (2): 71–82.

Fama, E. F., and K. R. French. 2015. "A Five-Factor Asset Pricing Model." *Journal of Financial Economics* 116 (1): 1–22.

Fiordelisi, F., M.-G. Soana, and P. Schwizer. 2013. "The Determinants of Reputational Risk in the Banking Sector." *Journal of Banking & Finance* 37 (5): 1359–1371.

Garg, P. 2020. ": Cybersecurity Breaches and Cash Holdings: Spillover Effect." *Financial Management* 49: 503–519.

Garg, A., J. Curtis, and H. Halper. 2003. ": The Financial Impact of IT Security Breaches: What Do Investors Think?" *Information Systems Security* 12: 22–33.

Gatzlaff, K. M., and K. A. McCullough. 2010. "The Effect of Data Breaches on Shareholder Wealth." *Risk Management and Insurance Review* 13 (1): 61–83.

Goel, S., and H. A. Shawky. 2009. "Estimating the Market Impact of Security Breach Announcements on Firm Values." *Information & Management* 46: 404–410.

Goins, S., and T. S. Gruca. 2008. "Understanding Competitive and Contagion Effects of Layoff Announcements." *Corporate Reputation Review* 11 (1): 12–34.
Gordon, L. A., M. P. Loeb, and L. Zhou. 2011. ": The Impact of Information Security Breaches: Has There Been a Downward Shift in Costs?" *Journal of Computer Security* 19: 33–56.
Haislip, J., K. Kolev, R. Pinsker, and T. Steffen. 2019. *The Economic Cost of Cybersecurity Breaches: A Broad-based Analysis*. Working Paper. Florida Atlantic University.
Higgs, J. L., R. E. Pinsker, T. J. Smith, and G. R. Young. 2016. "The Relationship Between Board-Level Technology Committees and Reported Security Breaches." *Journal of Information Systems* 30 (3): 79–98.
Hinz, O., M. Nofer, D. Schiereck, and J. Trillig. 2015. "The Influence of Data Theft on the Share Prices and Systematic Risk of Consumer Electronics Companies." *Information & Management* 52: 337–347.
Hovav, A., and J. D'Arcy. 2003. "The Impact of Denial-of-Service Attack Announcements on the Market Value of Firms." *Risk Management and Insurance Review* 6 (2): 97–121.
Hovav, A., and J. D'Arcy. 2005. "Capital Market Reaction to Defective IT Products: The Case of Computer Viruses." *Computers & Security* 24: 409–424.
Hovav, A., and P. Gray. 2014. "The Ripple Effect of an Information Security Breach Event: A Stakeholder Analysis." *Communications of the Association for Information Systems* 34: 893–912.
Jeong, C. Y., S.-Y. T. Lee, and J.-H. Lim. 2019. "Information Security Breaches and IT Security Investments: Impacts on Competitors." *Information & Management* 56 (5): 681–695.
Kamiya, S., J.-K. Kang, J. Kim, A. Milidonis, and R. M. Stulz. 2021. "Risk Management, Firm Reputation, and the Impact of Successful Cyberattacks on Target Firms." *Journal of Financial Economics* 139 (3): 719–749.
Kannan, K., J. Rees, and S. Sridhar. 2007. ": Market Reactions to Information Security Breach Announcements: An Empirical Analysis." *International Journal of Electronic Commerce* 12 (1): 69–91.
Kashmiri, S., C. D. Nicol, and L. Hsu. 2017. ": Birds of a Feather: Intra-Industry Spillover of the Target Customer Data Breach and the Shielding Role of IT, Marketing, and CSR." *Journal of the Academy of Marketing Science* 45: 208–228.
Kaspereit, T., K. Lopatta, S. Pakhchanyan, and J. Prokop. 2017. ": Systemic Operational Risk: Spillover Effects of Large Operational Losses in the European Banking Industry." *Journal of Risk Finance* 18 (3): 252–267.
Kelton, A. S., and R. R. Pennington. 2020. "Do Voluntary Disclosures Mitigate the Cybersecurity Breach Contagion Effect?" *Journal of Information Systems* 34 (3): 133–157.
Lang, L. H. P., and R. M. Stulz. 1992. "Contagion and Competitive Intra-Industry Effects of Bank-Ruptcy Announcements." *Journal of Financial Economics* 32 (1): 45–60.
Leong, Y.-Y., and Y.-C. Chen. 2020. "Cyber Risk Cost and Management in IoT Devices-Linked Health Insurance." *Geneva Papers on Risk and Insurance – Issues and Practice* 45 (4): 737–759.
Malhotra, A., and C. Kubowicz Malhotra. 2011. ": Evaluating Customer Information Breaches as Service Failures: An Event Study Approach." *Journal of Service Research* 14 (1): 44–59.
Marquardt, D. W. 1970. "Generalized Inverses, Ridge Regression, Biased Linear Estimation, and Nonlinear Estimation." *Technometrics* 12 (3): 591–612.
Martin, K. D., A. Borah, and R. W. Palmatier. 2017. ": Data Privacy: Effects on Customer and Firm Performance." *Journal of Marketing* 81: 36–58.
Mason, C. H., and W. D. Perreault. 1991. "Collinearity, Power, and Interpretation of Multiple Regression Analysis." *Journal of Marketing Research* 28 (3): 268–280.
McShane, M., and T. Nguyen. 2020. "Time-Varying Effects of Cyberattacks on Firm Value." *Geneva Papers on Risk and Insurance – Issues and Practice* 45 (4): 580–615.
Modi, S. B., M. A. Wiles, and S. Mishra. 2015. ": Shareholder Value Implications of Service Failures in Triads: The Case of Customer Information Security Breaches." *Journal of Operations Management* 35: 21–39.
Morse, E. A., V. Raval, and J. R. Wingender. 2011. ": Market Price Effects of Data Security Breaches." *Information Security Journal: A Global Perspective* 20: 263–273.
National Conference of State Legislatures (NCSL). 2020. *Security Breach Notification Laws*. Accessed July 6, 2020. www.ncsl.org.
Pirounias, S., D. Mermigas, and C. Patsakis. 2014. ": The Relation Between Information Security Events and Firm Market Value, Empirical Evidence on Recent Disclosures: An Extension of the GLZ Study." *Journal of Information Security and Applications* 19: 257–271.
Ponemon Institute. 2019. *2018 Cost of Data Breach Study: Impact of Business Continuity Management*. Accessed January 15, 2021. www.all-about-security.de.
Poyraz, O. I., M. Canan, M. McShane, C. A. Pinto, and T. S. Cotter. 2020. ": Cyber Assets at Risk: Monetary Impact on U.S. Personally Identifiable Information Mega Data Breaches." *Geneva Papers on Risk and Insurance – Issues and Practice* 45 (4): 616–638.
Privacy Rights Clearinghouse (PRC). 2018. *Data Breach Notification in the United States and Territories*. Accessed July 6, 2020. https://privacyrights.org.
Sinanaj, G., and J. Muntermann. 2013. "Assessing Corporate Reputational Damage of Data Breaches: An Empirical Analysis." *Proceedings of the 26th International Bled eConference*, 78–89.
Spanos, G., and L. Angelis. 2016. ": The Impact of Information Security Events to the Stock Market: A Systematic Literature Review." *Computers & Security* 58: 216–229.

Wheatley, S., A. Hofmann, and D. Sornette. 2021. "Addressing Insurance of Data Breach Cyber Risks in the Catastrophe Framework." *Geneva Papers on Risk and Insurance – Issues and Practice* 46 (1): 53–78.
World Economic Forum. 2016. *Understanding Systematic Cyber Risk: Global Agenda Council on Risk and Resilience*. White Paper.
Xie, X., C. Lee, and M. Eling. 2020. ": Cyber Insurance Offering and Performance: An Analysis of the U.S. Cyber Insurance Market." *Geneva Papers on Risk and Insurance – Issues and Practice* 45: 690–736.
Xu, M., K. M. Schweitzer, R. M. Bateman, and S. Xu. 2018. "Modeling and Predicting Cyber Hacking Breaches." *IEEE Transactions on Information Forensics and Security* 13 (11): 2856–2871.
Yayla, A. A., and Q. Hu. 2011. ": The Impact of Information Security Events on the Stock Value of Firms: The Effect of Contingency Factors." *Journal of Information Technology* 26: 60–77.
Yu, T., M. Sengul, and R. H. Lester. 2008. ": Misery Loves Company: The Spread of Negative Impacts Resulting from an Organizational Crisis." *Academy of Management Review* 33 (2): 452–472.
Zafar, H., M. S. Ko, and K.-W. Osei-Bryson. 2012. "Financial Impact of Information Security Breaches on Breached Firms and Their Non-Breached Competitors." *Information Resources Management Journal* 25 (1): 21–37.

Appendix

Table A1. Empirical evidence on cyber risk events.

Authors	Data				Methodology		Empirical results (CARs)[a]
	Source	Period	Type of cyber incident	Industry	Model	Estimation/event window	
Campbell et al. (2003)	*Wall Street Journal*, *New York Times*, *Washington Post*, *Financial Times*, *USA Today*	1995–2000	43 information security breaches	Publicly traded US firms	• Market model (NSYE/AMEX/NASDAQ) • SUR model	[-121;-2] [-1;1]	Significant negative
Hovav and D'Arcy (2003)	Lexis-Nexis	01/01/1998–06/30/2002	23 denial-of-service attacks	Firms publicly traded on NYSE, NASDAQ	• Market model (S&P500)	[-201;-2] [-1;0], [-1;1], [-1;5], [-1;10], [-1;25]	Insignificant negative
Cavusoglu, Mishra, and Raghunathan (2004)	Lexis-Nexis, CNET, ZDNET	1996–2001	66 internet security breaches	Publicly traded US firms	• Market model (NASDAQ composite index)	[-160;-1] [0;1]	Significant negative
Hovav and D'Arcy (2005)	Lexis-Nexis	1998–2002	186 public virus announcements	IT vendors traded on NYSE, NASDAQ	• Market model (S&P500)	[-201;-2] [0], [0;1], [0;5], [0;10], [0;25]	Insignificant negative
Kannan, Rees, and Sridhar (2007)	*Wall Street Journal*, *New York Times*, ZDNet, CDNET	1997–2003	72 information security breaches	Firms publicly traded on NYSE, AMEX, NASDAQ, OTCBB	• Market model (S&P500)	[-1;2], [-1;7], [-1;29]	Insignificant negative
Goel and Shawky (2009)	Public sources such as Lexis-Nexis, *Wall Street Journal*, *PC Week*, *The Register*, etc.	2004–2008	168 security breaches	Publicly traded US firms	• Market model • Fama-French three-factor • model	255 days [-119;10]	(Significant) negative
Gatzlaff and McCullough (2010)	Lexis-Nexis, Privacy Rights Clearinghouse	2004–2006	77 data breaches of customers and employees	Publicly traded firms	• Market model (value- and equally weighted CRSP, S&P500 weighted CRSP, S&P500)	[-252;-7] 18 different event windows	(Significant) negative
Gordon, Loeb, and Zhou (2011)	*Financial Times*, *New York Times*, *USA Today*, *Wall Street Journal*, *Washington Post*	1995–2007	121 information security breaches (4 types)	Publicly traded firms	• CAPM model (NYSE/AMEX/NASDAQ) • Fama-French three-factor model	[-121;-2] [-1;1], 7 days	Significant negative
Malhotra and Kubowicz Malhotra (2011)	DLDOS, Lexis-Nexis, *Wall Street Journal*	2000–2007	93 customer security breaches	Firms publicly traded on NYSE, AMEX, NASDAQ	• Market model (S&P500) • Carhart four-factor model	Variations of estimation and event windows	Significant negative/ positive

Morse, Raval, and Wingender (2011)	DataLossDB	01/10/2000–02/17/2010	306 data security breaches	Publicly traded firms	• Market model (value-weighted CRSP)	[-505;-251] 8 event windows	Significant negative
Yayla and Hu (2011)	Google, Yahoo, Lexis-Nexis	1994–2006	123 information security breaches (3 types)	Firms publicly traded on NASDAQ, NYSE, AMEX	• CAPM model (equally weighted NYSE/AMEX/NASDAQ)	[-130;-10] [-1;1], [-1;5], [-1;10]	(Significant) negative
Sinanaj and Muntermann (2013)	DataLossDB	2004–2011	72 data breaches	International listed firms (USA, GB, Russia, Japan, China, Germany)	• Market model (S&P500, FTSE100, DAX, Nikkei225, SSE Composite, S&P/ASX)	[-100;-50] [-5;-1], [0;1], [0;2], [0;3], [0;4], [0;5]	(Significant) negative
Pirounias, Mermigas, and Patsakis (2014)	DataLossDB, Identity Theft Report Center, Privacy Rights Clearinghouse, CNET, ZDNET	2008–2012	105 information security breaches	Publicly traded firms	• CAPM model • (Russell 3000) • Fama-French three- • factor model	[-201;-2] [-1,1], [-1,0], [0,0], [0,1]	(Significant) negative/ positive
Hinz et al. (2015)	DataLossDB, attrition.org, www.pressdisplay.com	04/26/2011–08/09/2012	6 data thefts	Software and hardware developers (publicly traded)	• Market model (S&P Global 1200, S&P500, Europe 350, S&P Japan 500)	[-200;-30] [-3;-1], [0], [0;1], [0;2], [0;3], [0;5], [-10;10]	(Significant) negative
Modi, Wiles, and Mishra (2015)	ITRC database, Factiva database	2005–2010	146 customer information security breaches (2 types)	Publicly traded firms	• Carhart four-factor model	[-1;1], [-2;2], [-1,0], [0,1]	Significant negative
Amir, Levi, and Livne (2018)	Audit Analytics cyberattack database, VCDB VERIS database	2010–2015	156 disclosed and withheld data breaches	Publicly traded US firms	• Risk-adjusted return	[-1;3], [-1;30]	(Significant) negative
McShane and Nguyen (2020)	Privacy Rights Clearinghouse, Lexis-Nexis, Google	2007–2016	536 cyberattacks	Publicly traded US firms	• One-factor model • Fama-French three-factor model • Carhart four-factor model • Buy-and-hold AR	[-300;-50], 11 event windows	(Significant) negative
Kamiya et al. (2021)	Privacy Rights Clearinghouse, Factiva, *Dow Jones Newswires*, news and business sources, *Presswire*, *Reuters* newswires, *Wall Street Journal*	2005–2017	165 data breaches	Publicly traded US firms	• Market model (value- and equally weighted CRSP) • Fama-French three- and Carhart four-factor model	[-280;-61] [-1;1], [-2;2], [-5;5]	Significant negative

[a]If more event windows are considered, the term 'significant' is presented in brackets for instances where not all cumulative abnormal returns/buy-and-hold abnormal returns are significant for all considered event windows. // The empirical studies are sorted by year of publication. In cases where more articles are published within one year, the author names were sorted alphabetically.

Table A2. Empirical evidence with respect to spillover effects from cyber risk events.

Authors	Data				Methodology		Empirical results[a] (CARs) with respect to spillover effects
	Source	Period	Type of cyber incident	Inter-/intra-industryspillover	Model	Estimation/event window	
Ettredge and Richardson (2003)	Keynote	02/07/2000–02/09/2000	4 denial-of-service attacks on internet firms	97 internet firms from Internet Stock List; 168 firms from 7 other industries	• Market model (NASDAQ)	[-300;-45] [1;3]	Significant negative/ positive
Garg, Curtis, and Halper (2003)	*Bloomberg*, *Dow Jones Interactive* (DJI)	1996–2002	22 IT security breaches	E-security vendors, P&C insurance carriers		[0], [0;1], [0,2]	(Significant) negative/ positive
Cavusoglu, Mishra, and Raghunathan (2004)	Lexis-Nexis, CNET, ZDNET	1996–2001	66 internet security breaches	Security developers	• Market model (NASDAQ composite index)	[-160;-1] [0;1]	Significant positive
Aytes, Byers, and Santhanakrishnan (2006)	Lexis-Nexis	1995–2005	67 information security breaches	Peer firms	• Market model (value-weighted NYSE, AMEX, NASDAQ)	[-165;-46] [-2;2]	Significant negative/ positive
Chen et al. (2012)	Data Loss Archive and Database (Attrition.org)	2006–2007	83 US breaches	10 IT consulting firms	• - Market model (NYSE)	[-120;-1] [0;1]	Significant negative/ positive
Hovav and Gray (2014)		01/17/2007	TJX attack	4 peer firms (Kohl's, Macy's, Target, Ross)	• Market model for TJX attack/ theoretical stakeholder analysis and key figures		(Negative)
Hinz et al. (2015)	DatalossDB, attrition.org, www.pressdisplay.com	04/26/2011–08/09/2012	6 data thefts from consumer electronic companies	62 peer firms	• Market model (S&P Global 1200, S&P500, Europe 350, S&P Japan 500)	[-200;-30] [-3;-1], [0], [0;1], [0;2], [0;3], [0;5], [-10;10]	(Significant) negative
Kashmiri, Nicol, and Hsu (2017)	S&P Compustat Database	12/09/2013	1 customer data breach of Target	168 publicly traded US retail firms	• Market model • Market adj. model	[-300;-46], [-250;-30] [-5;5], [0], [0;1], [0;2], [0;3], [0;4], [0;5], [0;6]	Significant negative

Martin, Borah, and Palmatier (2017)	Capital IQ, Factiva, Lexis-Nexis, Privacy Rights Clearinghouse		293 data security breaches (199 global publicly traded firms)	176 peer firms	• Market model (NYSE, Paris stock exchange, LSE)	[-1;1], [-1;0], [0], [0;1]	(Significant) negative
Haislip et al. (2019)	Audit Analytics	01/2010–03/2018	353 breaches (248 unique firms)	11,508 non-breached peers; 19,917 insurers (cyber and non-cyber insurance firms)	• Buy-and-hold abnormal return (BHAR) as depend variable	[-1;1], [-2;2], [-5;5], [-5;10]	Significant negative buy-and-hold abnormal returns
Jeong, Lee, and Lim (2019)	Privacy Rights Clearinghouse, DataLossDB, Heritage Foundation, Identity Theft Resource Center	2010–2017	118 information security breaches	823 peer firms	• Market model (S&P 500)	180 days, [-2;2], [-1;1], [0;1], [0,2]	Significant positive
Kamiya et al. (2021)	Privacy Rights Clearinghouse, Factiva, *Dow Jones Newswires*, news and business sources, press release wires, *Reuters* newswires, *Wall Street Journal*	2005–2017	165 data breaches of publicly traded US firms	146 industry peer firms; 6,094/5,775 individual industry peer firms	• Market model (value- and equally weighted CRSP)	[-280;-61] [-1;1], [-2;2], [-5;5]	Significant negative

Table A2. Empirical evidence with respect to spillover effects from cyber risk events (continued).

Authors	Data				Methodology	Empirical results with respect to spillover effects
	Source	Period	Type of cyber incident	Inter-/intra-industry spillover	Model	
Zafar, Ko, and Osei-Bryson (2012)	Lexis-Nexis Academic Database	1997–2007	119 information security breaches	867 peer firms	• Performance ratios	Intra-industry information transfer for specific security breach types and the presence of contagion effects
Baldwin et al. (2017)	Industry Standard SANS Data	01/2003–02/2011	10 IP services		• Vector equation system	Contagion effects from cybersecurity attacks
Corbet and Gurdgiev (2019)	Lexis-Nexis	01/01/2005–04/30/2015	819 cybercrime and hacking events	Financial markets	• EGARCH model (volatility effects)	Stock price volatility and contagion effects for different types of cybercrime
Garg (2020)	Privacy Rights Clearinghouse	2005–2017	103 breaches of parent firms; 75 breaches of unlisted subsidiaries	Peer firms, suppliers	• Regression with cash holdings as depend. variable	Increasing cash holdings of companies that experienced cybersecurity breaches, their peer firms and suppliers
Kelton and Pennington (2020)			Cybersecurity breach	Non-professional investors	• Single factor between participants experiment with non-professional investors	Strong contagion effects; cybersecurity disclosures prior to the event announcement can mitigate contagion effects.
Caporale et al. (2021)	www.hackmageddon.com	08/12/2015–01/15/2020	4,693 cyberattacks	Cryptocurrency market	• VAR-GARCH (1,1) process	Cyberattacks intensify linkages across markets and decrease portfolio diversification options for investors of cryptocurrencies.

[a]If more event windows are considered, the term 'significant' is presented in brackets for instances where not all cumulative abnormal returns/buy-and-hold abnormal returns are significant for all considered event windows.

Table A3. Top 10 data breaches (based on the number of breached records).

Date made public	Company	Breach type	Total number of breached records
09/07/2017	Equifax Corporation	HACK	145,500,000
01/20/2009	Heartland Payment Systems[a]	HACK	130,000,000
02/05/2015	Anthem	HACK	80,000,000
08/28/2014	J.P Morgan Chase	HACK	76,000,000
08/02/2008	Countrywide Financial Corp.[a]	INSD	17,000,000
03/26/2008	Bank of New York Mellon	PORT	12,500,000
07/03/2007	Fidelity National Information Services	INSD	8,500,000
03/30/2012	Global Payments Inc.	CARD	7,000,000
09/14/2007	TD Ameritrade Holding Corp.	HACK	6,300,000
01/06/2009	CheckFree Corp.[b]	HACK	5,000,000

[a]Heartland Payment Systems was acquired by Global Payments in 2016, and Countrywide Financial Corp. was acquired by Bank of America in 2008.
[b]CheckFree has been part of Fiserv since 2007.