Gatzert, Nadine; Schubert, Madeline

Cyber risk management in the US banking and insurance industry: A textual and empirical analysis of determinants and value

Journal of Risk and Insurance

Provided in Cooperation with:
John Wiley & Sons

Suggested Citation: Gatzert, Nadine; Schubert, Madeline (2022) : Cyber risk management in the US banking and insurance industry: A textual and empirical analysis of determinants and value, Journal of Risk and Insurance, ISSN 1539-6975, Wiley, Hoboken, NJ, Vol. 89, Iss. 3, pp. 725-763, https://doi.org/10.1111/jori.12381

Received: 7 May 2020 | Revised: 3 April 2022 | Accepted: 7 April 2022

DOI: 10.1111/jori.12381

ORIGINAL ARTICLE

Journal of Risk and Insurance

Cyber risk management in the US banking and insurance industry: A textual and empirical analysis of determinants and value

Nadine Gatzert | **Madeline Schubert**

School of Business, Economics and Society, Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU), Nürnberg, Germany

Correspondence
Madeline Schubert, School of Business, Economics and Society, Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU), Lange Gasse 20, 90403 Nürnberg, Germany.
Email: madeline.schubert@fau.de

Funding information
Faculty of Business, Economics and Law at Friedrich-Alexander-Universität Erlangen-Nürnberg,
Grant/Award Number: Faculty Women's Prize

Abstract

In this paper, we first construct a cyber risk consciousness score using a text mining algorithm, applied to annual reports of large- and mid-cap US banks and insurers from 2011 to 2018. We next categorize the firms' cyber risk management based on keywords to study determinants and value-relevance. Our results show an increasing cyber risk consciousness, regardless of the industry. In addition, for the entire sample we find that firms belonging to the banking industry, with a higher cyber risk consciousness score and a higher general risk awareness are more likely to implement cyber risk management, which also holds for both industries separately. We find the opposite in the case of profitable firms for the entire sample and the insurer subsample. Finally, we observe a significant positive relationship between cyber risk management and firm value measured by Tobin's Q for the entire sample and the subsamples of banks and insurers.

KEYWORDS
cyber (security) risk management, cyber risk, cybersecurity, text mining

JEL CLASSIFICATION
G21, G22, G32, K24

1 | INTRODUCTION

Cyber risk events can cause considerable and manifold consequences for affected enterprises. In the Allianz Risk Barometer 2019 and 2020, cyber risk was ranked as the most important global business risk, together with business interruption primarily triggered by cyber risk incidents. At the same time, US authorities and regulators discuss Enhanced Cyber Risk Management Standards (see the Basel Committee on Banking Supervision (Basel Committee on Banking Supervision [BCBS], 2018). Against this background, corporate decisions regarding the implementation and continuous improvement of cyber risk management (CyberRM) play a crucial role. Since the awareness of risks is a vital prerequisite for managing them (see Berkman et al., 2018), we first construct a cyber risk *consciousness* score based on a rules-based text mining algorithm that is applied to the annual reports of US banks and insurers from 2011 to 2018. Second, based on annual reports we identify whether and to what extent cyber risk *management* is implemented and then empirically study the determinants and value of having CyberRM in place, depending on the respective industry.

There is currently no standardized definition of cyber risk, with a variety of concretizations in the literature (see, e.g., Biener, Eling, Matt, et al., 2015; Biener, Eling, & Wirfs, 2015; Eling & Schnell, 2016; Eling et al., 2021; Shetty et al., 2018). Empirical studies regarding cyber risks mainly focus in the market reactions of data, information, and internet security breaches, or specific methods of attack, such as denial-of-service attacks (see, e.g., Gatzlaff & McCullough, 2010). Kamiya et al. (2021) additionally examine the implications of cyberattacks on target firms' reputation, risk management and possible contagion effects. With respect to cyber risk management, Pooser et al. (2018) focus on cyber risk identification and the perception of US property and casualty insurers, whereas Shetty et al. (2018) study the usefulness of a cyber risk scoring and mitigation tool, enabling enterprises to improve decision-making concerning mitigation policies. Berkman et al. (2018) investigate cybersecurity awareness and the resulting (positive) market valuations for 10-K disclosures of (nonfinancial) US firms from 2012 to 2016.

The determinants and value of CyberRM in the banking and insurance industry have seldom been the focus of the literature to date, even though cyber risks are of particular relevance for this industry due to the sensitive data they hold. In this paper, we aim to fill this gap by providing a textual and empirical analysis of the US banking and insurance industry regarding awareness, determinants and value of CyberRM, which, to the best of our knowledge, has not been examined in such great detail to date. We first construct a cyber risk consciousness score by developing a rules-based text mining algorithm based on the sample firms' annual reports from 2011 to 2018, thereby extending the approach in Berkman et al. (2018). In line with their nonfinancial industry study for the period 2012 to 2016, our results show an increasing cyber risk consciousness score in the US banking and insurance industry over the sample period, with US insurers registering (significantly) higher mean scores by comparison with US banks.

Second, we develop a keyword catalogue to identify three levels of CyberRM based on annual reports. We conduct a logistic regression to study the determinants of CyberRM and a treatment-effects model with maximum-likelihood estimates to investigate the value-effect of CyberRM on Tobin's Q. Our regression analysis shows that US banks with a higher cyber risk awareness and a higher level of risk awareness are more likely to implement CyberRM when considering all firms within the sample, whereas profitable firms are less likely to adopt

CyberRM. When examining US banks and insurers separately, we still observe a positive relationship between cyber risk awareness as well as risk awareness and CyberRM for both subsamples. With respect to US insurers, we additionally find that profitable firms are less likely to adopt CyberRM. Finally, we observe a statistically significant positive effect of CyberRM on firm value in both the US banking and insurance industry.

Overall, our analysis is the first to study the awareness, determinants and value of CyberRM in the US banking and insurance industry, which in the future will be of even greater relevance for firms, board members, clients and policymakers against the background of regulatory and technological data-driven developments.

The paper is structured as follows. Section 2 introduces the hypotheses development, methodology and data sample, Section 3 presents the textual and empirical results regarding the cyber risk awareness, determinants and value of CyberRM, and Section 4 summarizes the paper.

2 | DEVELOPMENT OF HYPOTHESES, METHODOLOGY, AND DATA SAMPLE

2.1 | Definitions and theoretical relevance of cyber risk management

We follow the approach of previous literature as well as insurance regulators, and define cyber risk as a subcategory of operational risk. For example, Biener, Eling, and Wirfs (2015, p. 133) define (operational) cyber risks as "operational risks to information and technology assets that have consequences affecting the confidentiality, availability or integrity of information or information systems" (in line with Cebula & Young, 2010, p. 1).[1] A glossary of essential definitions and cybersecurity terminology is provided by the National Initiative for Cybersecurity Careers and Studies (NICCS, 2018), for instance. With respect to CyberRM, Biener, Eling, Matt, et al. (2015) as well as Eling and Schnell (2016), recommend the use of information security standards, such as the ISO 27001 standard, the IT Governance Framework COBIT or the US NIST Framework (see also BCBS, 2018; Higgs et al., 2016; Marotta & McShane, 2018). For a review of research on the respective process steps of cyber risk management, we refer to Eling et al. (2021).

Regarding the theoretical relevance of (cyber) risk management, Kamiya et al. (2021) argue that firm value depends on a concave profit function and decreases with a rising volatility of profits, when holding the mean constant. In this case, despite its costs, risk management can be valuable if it contributes to the reduction of profit volatility, depending on various factors (see, e.g., Froot et al., 1993; Kamiya et al., 2021). Defining cyber risk as an operational risk and thus by a loss distribution, costly risk management and mitigation measures can reduce the respective exposure. For this reason, Kamiya et al. (2021) anticipate more investments in (cyber) risk management, when the implications of a cyberattack are more costly for firms. The relevance of implementing cyber risk management is also emphasized by the empirical study in Xie et al. (2020), who find that offering standalone cyber insurance products is risky even for insurers as reflected in higher loss ratios as compared to packaged products, which is due to the nature of cyber risk as a highly dynamic risk with catastrophic loss potential, high information asymmetry and a lack of sufficient data.

[1]There is also an overlap with the definition of *IT risk*, which stems from the vulnerabilities of a firm's physical IT assets (Biener, Eling, Matt, et al., 2015; Biener, Eling, & Wirfs, 2015) or a cybersecurity component (Higgs et al., 2016) and can be understood in a broader sense as an "information security risk or risk resulting in failure of information systems" (Biener, Eling, & Wirfs, 2015, p. 132).

2.2 | Textual approach regarding the cyber risk (management) awareness

As the awareness of cyber risks is a vital prerequisite for risk management, we first develop a cyber risk consciousness score by extending the approach in Berkman et al. (2018), who introduce a firm-specific cybersecurity awareness measure based on 10-K reports. We use the text mining extension of the predictive analytics software RapidMiner and apply the process laid out in the upper section of Table 1.

Our original dictionary for the text mining process contains the glossary of common cybersecurity terminology published by the NICCS (2018) and the US federal laws relating to cybersecurity from the Congressional Research Service (see Fischer, 2014; e.g., the Health Insurance Portability and Accountability Act of 1996 and the Gramm-Leach-Bliley Act of 1999).[2] In addition to these regulations and the terminology associated with "cybersecurity," we also include the terms "cyber," "cyber (security) risk," and "cyber (security) risk management" in our initial list of words and phrases.[3]

Based on this list of words and phrases, we next generate eleven independent dictionaries of so-called n-grams: for example, the first dictionary contains 109 single words (1-grams), the second dictionary includes 108 phrases consisting of two words (2-grams), the third dictionary includes 90 phrases of 3 words (3-grams), until the 11th dictionary, which contains phrases of 11 words, the longest possible phrase in our setting (see also Loughran & McDonald, 2016 for this process, and the references therein).

We then tokenize the annual reports of the firms, transform the text into lowercase and apply a stemming algorithm to obtain the root words and control for plural forms. After running the RapidMiner process for every firm and fiscal year separately, we compute the firm-specific cyber risk consciousness score by summing up the number of words and phrases identified in the annual reports for all n-grams over the entire observation period (see formula in Table 1), thereby avoiding double counting. Furthermore, we excerpt the word counts of the term "risk" and the total number of words per document to compute relative frequencies.

The validation of the algorithm is presented in the lower section of Table 1, which is an iterative process to improve the accuracy and precision of the text mining output. Despite certain limitations of the text mining approach using a RapidMiner process,[4] a manual

[2]By comparison with Berkman et al. (2018), we also consider the relevant regulations for US banks and insurers, which became effective after 2014 and were identified through our initial screening process of the annual reports. For insurers, these regulations include the National Association of the Insurance Commissioners (NAIC) Cybersecurity Bill of Rights of 2015 as well as the NAIC Insurance Data Security Model Law of 2017, and for banks the Enhanced Cyber Risk Management Standards of 2016. We further take into account US state-specific security breach notification laws from the National Conference of State Legislatures NCSL, (2020), in particular the New York Department of Financial Services (NYDFS) Cybersecurity Regulation of 2018, the South Carolina Security Bill and the California Consumer Privacy Act (CCPA) of 2018. Moreover, report-specific regulations are included with the Securities and Exchange Commission (SEC) Cybersecurity Disclosure Guidance from 2011 and the update in 2018 as well as other regulations such as the Cybersecurity Information Sharing Act (CISA) of 2015.

[3]See also Heidinger and Gatzert (2018) for this approach in the context of reputation risk management. To avoid double counting, e.g., as the counts for "cyber" also contain "cyber (security) risk" and "cyber (security) risk management" and the counts for "cyber (security) risk" are contained within "cyber (security) risk management," we made respective adaptions as proposed by Heidinger and Gatzert (2018).

[4]One disadvantage of a text mining approach is that the output solely indicates the total number of matches with pre-defined words, whereas the context in relation to other words is ignored. While this is not an issue when deriving the cyber risk consciousness score, due to the consideration of the n-grams of words/phrases, this is not feasible when aiming to identify a

TABLE 1 Description of text mining procedure and validation of results.

Development of cyber risk consciousness score

- Construction of 11 independent dictionaries based on initial collection of 109 words (1-grams) and 334 phrases (divided into dictionaries with 2-grams (phrases of two words), 3-grams (phrases of three words), ..., 11-grams (phrases of 11 words)) with respect to cyber (security) risk management (see Fischer, 2014; Heidinger & Gatzert, 2018; National Conference of State Legislatures [NCSL], 2020; National Initiative for Cybersecurity Careers and Studies [NICCS], 2018)
- Storage of the 11 independent dictionaries as *.txt documents
- Set up of a process with the text mining extension of RapidMiner to read the SEC disclosures (*.txt) and compare content with the dictionaries, applying the following steps to annual reports and dictionaries:
  - Tokenize the text and transform it into lower case
  - Apply Porter's stemming algorithm (if phrases consist of two or more words)
  - Generate different patterns of n-grams by varying the maximum length between 1 and 11
  - Extract the total number of matches with the respective keywords/phrases and disclosures
  - Repeat this process for every dictionary separately, to identify different n-grams
- Computation of cyber risk consciousness score = Σ(1-grams) + ... + Σ(11-grams)

Validation of text mining results

- Transparent and controllable text mining process, due to the possibility of comparing content from selected SEC annual reports by means of a search function, with text mining output from RapidMiner, as the total number of hits are disclosed for each word/phrase and annual report separately[a]
- Manual validation and review of noticeable text mining results during score processing (e.g., significantly high hit rates) followed by adaptions to enhance the precision of word/phrase count extraction:
  - Adjustments of dictionaries should the included words/phrases have a high hit rate, with a low, specific focus on cyber (security) risk awareness, i.e., removed: “asset,” “event,” “exposure,” “impact,” “risk,” “subject,” “risk analysis,” “risk assessment,” “risk management,” “risk mitigation,” “enterprise risk management” and “integrated risk management” (see Berkman et al., 2018)
  - Porter's stemming algorithm in relation to single words (1-grams) is not applied, as the results are less accurate[b]
  - Cross-checking of the correct extraction of state breach notification laws with respect to article numbers, since non-letters are removed through tokenization
- Additional cross-check of the accuracy of the text mining process by generating a.txt test file with a pre-defined number of keywords and phrases, to evaluate the correctness of the n-gram extraction process

[a]The text mining algorithm extracts the absolute number of the word sequences (n-grams) from the annual reports based on pre-defined wordlists, and does not make predictions based on mathematical models (see North, 2018, pp. 248–250).

[b]For instance, the word stems “avail” and “integr” have 89,955 and 13,372 hits from 2011 to 2018, respectively, whereas the relevant keywords “availability” and “integrity” actually occur 6434 and 1246 times, respectively.

examination of a large number of annual reports (in our case 992 disclosures) for the cyber risk consciousness score computation would be a more error-prone and an unstandardized procedure (see also Berkman et al., 2018; Heidinger & Gatzert, 2018).

CyberRM implementation. For instance, the hit of “cyber risk management” is a first indication of CyberRM but may also refer to the discussion of regulatory developments in annual reports, such as the “Enhanced Cyber Risk Management Standards.” Therefore, to assess whether CyberRM is implemented at the respective firm (and to what degree), an additional manual examination is needed (see Section 2.3). Another limitation arises from software implementation. For example, the occurrence of word phrases leads to unavoidable allocation problems, for example, the term “cyber” within “cyber and information risks,” is allocated to the term “cyber” instead of the “cyber risk” category.

Against the background of an increasing relevance of CyberRM, as emphasized by regulatory initiatives listed above, we expect a growing consciousness of CyberRM, as indicated by the increasing (mean) score over the sampling period.

2.3 | Keyword approach regarding cyber risk management

To determine whether a firm has CyberRM in place, we use context specific keywords in line with the empirical literature regarding the identification of enterprise risk management (ERM) (see, e.g., Hoyt & Liebenberg, 2011; Pagach & Warr, 2011) and reputation risk management programs (see Heidinger & Gatzert, 2018). Given that the financial services industry is highly regulated and supervised, we can generally assume a high level of transparency and quality of information regarding existing risks and their management within annual reports, which is further enhanced by specific reporting requirements (see, e.g., Securities and Exchange Commission SEC, 2011, 2018; in cases of cyber risks).

We distinguish between four cases regarding a CyberRM implementation, as shown in Table 2, where we take into account the relationship of cyber risk to IT, information security and operational risk. CyberRM = 1c describes a case in which cyber/IT or information security risks are treated as an own risk category in the annual report with an established definition, which we consider a strong indication of CyberRM. Second, CyberRM = 1b if the keywords and criteria derived from the literature (see Section 2.1) and presented in Table A1 are satisfied regarding an available framework/strategic guidelines and/or a committee or function responsible for dealing with cyber risks (e.g., a Chief Information Security Officer (CISO) as is often used in ERM literature), and/or specific pre-defined risk mitigation/transfer measures are in place, for example, the purchase of cyber insurance to manage cyber risks. Combinations of more criteria are possible and can be considered as representing a higher degree of implementation. Third, CyberRM = 1a if the cyber risk is not managed separately, but is integrated in the OpRM process ("cyber risk" or "cybersecurity risk" is mentioned in the OpRM section), without reporting on

TABLE 2 CyberRM levels.

CyberRM level	Criteria and keywords
CyberRM = 1c	Own risk category in the risk management section, with an established (comprehensive/deeper) definition of cyber/cybersecurity risk, IT risk or information security risk
CyberRM = 1b	Criteria and keywords in Table A1 are satisfied regarding the presence of framework/strategic guidelines, committee/function or cyber risk mitigation/transfer measures, but no specific cyber/cybersecurity/IT/information security risk category
CyberRM = 1a	Cyber risk is not managed separately, but integrated into operational risk management (OpRM) (if the term "cyber risk" or "cybersecurity risk" is mentioned in the OpRM section, but without specific risk management measures, e.g. "cyberattack," "cyber breach/incidents," and "cybercrime")
CyberRM = 0	None of the above

detailed CyberRM measures.[5] Table A2 provides excerpts of annual reports to demonstrate the procedure, where applicable keywords or phrases are displayed in italics.

2.4 | Hypotheses development

In the empirical analyses, we use *CyberRM* as the dependent variable and set it to 1 for the respective firm if the CyberRM level is 1a, 1b, and/or 1c as reflected in its annual report, and we differentiate between the respective CyberRM levels in the robustness tests. We then study the impact of the following determinants on CyberRM.

Size: In general, large companies are faced with an increasing number as well as complexity of risks (see Hoyt & Liebenberg, 2011; Nocco & Stulz, 2006). They also have considerable financial resources, rendering them more likely to implement an ERM system (see Hoyt & Liebenberg, 2011; Lechner & Gatzert, 2018; Pagach & Warr, 2011). These theoretical arguments from the ERM literature are similarly reasonable as regards a CyberRM implementation. Empirical research in the field of cyber risk reveals that firm size plays an important role regarding the occurrence of cyber risk incidents. Large companies with a higher number of employees suffer cyber losses more frequently (see Biener, Eling, & Wirfs, 2015). In this context, Cavusoglu et al. (2004) find that negative shocks such as internet security breaches are easier to handle in the case of larger companies due to more available resources, for example, highly skilled IT staff, which might be an indicator that larger firms have adequate CyberRM. Furthermore, Gatzlaff and McCullough (2010) find that large, publicly traded firms can better absorb the negative impact of a data breach in relation to the company's stock price, whereas Malhotra and Kubowicz Malhotra (2011) observe that larger firms experience a greater loss of market value following customer information breaches. Regarding financial firms, Ettredge et al. (2018) report a statistically significant positive relationship between firm size and the probability of a future breach incident, which is in line with the empirical findings regarding the occurrence of cyber incidents and firm size for various industry types (see, e.g., Higgs et al., 2016; Kamiya et al., 2021). However, Pooser et al. (2018) empirically show that small US property and casualty insurers, in particular, are "early adopters of cyber risk identification" (sample from 2006 to 2015), which is relevant for CyberRM. Given these considerations, we calculate firm size based on the natural logarithm of a firm's book value of total assets (see, e.g., Gordon et al., 2010; Hoyt & Liebenberg, 2011) and hypothesize:

H1: *Larger companies are more likely to implement CyberRM.*

Leverage: We also take into account the financial leverage of a company, measured by the ratio of its book value of total liabilities in relation to its market value of equity (see Bohnert, Gatzert, et al., 2019). Empirical insights in this context are ambiguous. While Higgs et al. (2016) identify a significant positive relationship between financial

[5]Note that if at least two CyberRM measures (see criteria in Table A1) are listed in an OpRM section, then we classify this firm in the category of CyberRM = 1b (and not in 1a), as this signals that cyber risk is managed "more specifically." However, we have also checked the results when categorizing firms that (only briefly) mention their understanding of cyber/cybersecurity risk, IT risk or information security risk in the forward-looking information and risk factor section or OpRM section and have assigned these firms to 1c, rather than 1b or 1a.

leverage and the occurrence of a cyber incident, Kamiya et al. (2021) observe a (significant) negative relationship, which could suggest the absence of CyberRM. Similarly, McShane and Nguyen (2020) find an insignificant negative association between financial leverage and stock market reactions to cyberattacks. By contrast, for their sample of US property and casualty insurers from 2006 to 2015, Pooser et al. (2018) find that more leveraged companies are early adopters of cyber risk identification. From a theoretical perspective, firms may implement risk management programs to counterbalance the potentially higher risk of financial distress resulting from higher leverage (see Bohnert, Gatzert, et al., 2019; Pagach & Warr, 2011). In this context, a stronger risk appreciation, as signaled by an implemented risk management program, might result in more favorable debt conditions (see Meulbroek, 2002; with a focus on companies from the US; Hoyt & Liebenberg, 2011; with focus on US insurers). Similarly, Kamiya et al. (2021) argue that the level of leverage might further increase after a cyberattack, as it would not be optimal for equity holders to increase their shares to benefit debtholders. This provides support for the establishment of CyberRM. Conversely, a higher leverage with a generally higher risk of financial distress might also lead to less resources, which are required to put an adequate program into practice (see Baxter et al., 2013). Overall, we thus hypothesize:

H2: *Companies with a higher financial leverage are more likely to implement CyberRM.*

Return on assets (RoA): According to Hoyt and Liebenberg (2011), more profitable firms (and thus those with more resources) are more likely to implement an ERM, whereby profitability is calculated by the RoA as the annual net income, relative to the book value of total assets (see Pooser et al., 2018). In addition, empirical studies show that more profitable firms frequently suffer from cyber losses (see Kamiya et al., 2021) and have a greater likelihood of belonging to the early adopters of cyber risk identification (see Pooser et al., 2018). In the case of financial firms, Ettredge et al. (2018) also observe a positive, but insignificant association between RoA and subsequent breach incidents. In line with this, we anticipate that enterprises with a higher RoA make more efforts to counter cyber risks and assume:

H3: *Companies with a higher RoA are more likely to implement CyberRM.*

CapitalOpacity: According to the ERM literature, a higher information asymmetry, associated with a higher portion of intangible assets and thus more opaqueness, might result in an undervaluation of a firm (see Hoyt & Liebenberg, 2011; Lechner & Gatzert, 2018; Pagach & Warr, 2011). ERM helps to overcome these issues by providing stakeholders with information regarding a firm's financial strength and risk profile (see Pagach & Warr, 2011). Following Hoyt and Liebenberg (2011), capital opacity is determined by the ratio of intangible assets in relation to the book value of total assets. In particular, Saunders and Brynjolfsson (2016, p. 84) point out that "IT intangibles are a significant driver of market value, even though they are 'invisible' on the balance sheet," and in case of data security breaches, intangible costs, due to a loss in consumer confidence, are likely to occur (see, e.g., Cavusoglu et al., 2004). Kamiya et al. (2021) also highlight that companies with more immaterial assets tend to suffer more from a cyberattack, and Ettredge et al. (2018) conclude that firms mentioning the existence of trade secrets, have a higher probability of suffering from cybersecurity breaches. Therefore, we hypothesize:

H4: *Companies with higher capital opacity are more likely to implement CyberRM.*

Bank: To study the potential differences[6] between banks and insurers, we include a dummy variable that is set to 1, if the observed firm belongs to the banking sector, based on the classification of Thomson Reuters Eikon. In general, reputational damages after a cyberattack announcement are costly and can result in firm stakeholders adversely changing their behavior (e.g., purchase less, demand other terms, see Heidinger & Gatzert, 2018; Kamiya et al., 2021). CyberRM should thus be of particular relevance for both banks and insurers due to the highly sensitive data they handle. In addition, the state security breach notification laws and the SEC Cybersecurity Disclosure Guidance hold for publicly listed US banks and insurers, requiring them to inform affected individuals about personal data breaches.[7] As can be seen from Tables A4–A6, the vast majority of US banks and insurers in the present sample underlie a data breach notification law during the entire sample period, except for three US banks in Florida where the state security breach notification law became effective in 2014 (9 out of 992 firm-year observations) and four US insurers[8] (32 out of 992 firm-year observations). However, the banking sector is more prone to systemic risk and spillover effects (e.g., also caused from cyber risk events) than the insurance industry (see Eling & Pankoke, 2016; Heidinger & Gatzert, 2018). For instance, insurance claims are typically limited to contractually defined events and are not as liquid (e.g., due to lapse penalties) as callable bank liabilities during a bank run (see Heidinger & Gatzert, 2018; Kessler, 2013). Against this background, banks should place even more focus on the implementation of CyberRM to reduce related reputation losses and to avoid negative spillover effects caused by other financial services companies. We hence assume:

H5: *Companies of the banking industry are more likely to implement CyberRM.*

CyberRiskAwareness: Using the cyber risk consciousness score (see Section 2.2) as an approximate measure for cyber risk awareness, based on the reporting behavior of US banks and insurers within annual reports, we anticipate that firms with a higher score are more concerned about cyber risk as also shown by Berkman et al. (2018). In robustness tests we additionally use a previously experienced cyberattack as an alternative proxy for "cyber risk awareness" and as an additional variable.[9] Overall, we assume:

H6: *Companies with a higher cyber risk awareness are more likely to implement CyberRM.*

[6]We examine both industries jointly by including an indicator variable as proposed by Heidinger and Gatzert (2018). As the value variables of H1 to H4 might differ across the US banking and insurance industry, we additionally investigate both industries separately in subsamples, in line with Cummins et al. (2006).

[7]The US security breach notification laws have been passed at state- and territory-level with different effective dates over a time period of 16 years, starting in California in July 2003 as the first US state and followed by all other 49 US states and territories until July 2018 (see Kamiya et al., 2021; National Conference of State Legislatures [NCSL], 2020).

[8]The jurisdiction of the incorporation or organization of four insurers is located outside the US according to their SEC annual reports in Form 10-K. Three of these have their headquarters in Bermuda, and the US insurer Chubb has identified Switzerland as its respective jurisdiction, see also Table A6.

[9]Berkman et al. (2018) use a technology committee and previous experience from cyber risk events as additional proxies for cybersecurity awareness. As the presence of a technology committee is an indicator of our dependent variable CyberRM we exclude this proxy.

RiskAwareness: Another variable we include in our regression analysis is the general risk awareness of the observed firms, following Heidinger and Gatzert (2018). We extract the absolute number of the term "risk" in annual reports using text mining, and assume that companies with more hits of this search term are exposed to a greater variety of risks. Additionally, these firms have an increased awareness and understanding of their risks leading to the deployment of appropriate (cyber) risk management measures (see Heidinger & Gatzert, 2018). We hence hypothesize:

H7: *Companies with a higher risk awareness are more likely to implement CyberRM.*

According to empirical research, cyber risk events such as security breaches can have considerably negative market value effects on the firms affected (see, e.g., Cavusoglu et al., 2004; Gatzlaff & McCullough, 2010; Kamiya et al., 2021), whereas the disclosure of information security in the annual reports is positively related to the market value of a firm (see Gordon et al., 2010). Therefore, we investigate the value-relevance of CyberRM following Hoyt and Liebenberg (2011) and Heidinger and Gatzert (2018) and using Tobin's *Q*, which is given as the sum of the market value of equity and the book value of liabilities, divided by the book value of the total assets. We assume:

H8: *Implementing CyberRM creates value for firms as measured by Tobin's Q.*

2.5 | Methodology

To investigate the determinants of CyberRM, we use a logistic regression as is done in Liebenberg and Hoyt (2003) and Lechner and Gatzert (2018) as well as Heidinger and Gatzert (2018), who study ERM and reputation risk management determinants, respectively, assuming

$$CyberRM = f\,(Size, Leverage, RoA, CapitalOpacity, Bank, CyberRiskAwareness, RiskAwareness). \tag{1}$$

We include year dummies (see also Berkman et al., 2018) and specify the model as

$$\begin{aligned} \ln\left(\frac{p(CyberRM=1)}{1-p(CyberRM=1)}\right) = {} & \beta_1 Size + \beta_2 Leverage + \beta_3 RoA + \beta_4 CapitalOpacity \\ & + \beta_5 Bank + \beta_6 CyberRiskAwareness \\ & + \beta_7 RiskAwareness + \beta_{8-14} YearDummies + \varepsilon. \end{aligned} \tag{2}$$

The logarithmized quotient on the left side of Equation (2) represents the likelihood that one of our observed firms has implemented CyberRM, which is denoted as $p(CyberRM = 1)$. We have also clustered standard errors at firm-level to prevent biases from dependencies of two or more firm-year observations of the same company (see Hoyt & Liebenberg, 2011; Petersen, 2009).

To study the value-relevance of CyberRM, we treat CyberRM as endogenous and use a treatment-effects model following Hoyt and Liebenberg (2011) as well as Bohnert, Fritzsche, et al. (2019), Bohnert, Gatzert, et al. (2019) in the ERM context. Besides considering CyberRM as our major independent variable, we additionally include the previously presented variables in Section 2.3 as firm value determinants in Section 2.3 as well as negative sentiment in annual reports ($Tone_{neg}$)

based on the analysis of Berkman et al. (2018), who find a negative relationship when examining cybersecurity awareness and market value.[10] The model is then described as a system of two equations, which are simultaneously estimated through maximum-likelihood (see Bohnert, Fritzsche, et al. 2019; Bohnert, Gatzert, et al., 2019; Hoyt & Liebenberg, 2011; Maddala, 1983).[11] First, the functional form of the regression (Q Equation) regarding the determinants of Tobin's Q can be described by

$$Q = f\,(CyberRM|Size, RoA, CapitalOpacity, Bank, Tone_{neg}). \tag{3}$$

second, the functional form of the selected CyberRM determinants ($CyberRM$ Equation) is given by

$$CyberRM = f\,(Size, Leverage, RoA, CapitalOpacity, CyberRiskAwareness, RiskAwareness). \tag{4}$$

(see, e.g., Hoyt & Liebenberg, 2011; or Bohnert, Gatzert, et al., 2019 for the formal description and Table A3 for a summary of all variables of the regression models, their measurement and expected sign).

2.6 | Data sample

For our empirical study, we extract all US banking and insurance firms from Thomson Reuters Eikon with a reported market capitalization on December 31, 2018 and then apply screening criteria as shown in Table 3.

Firstly, we exclude small-cap firms with a market capitalization below one billion USD on December 31, 2018, thus focusing on 203 mid- and large-cap banks and insurers in the US (reflecting 95.61% of total market capitalization), which might result in a possible selection bias. For instance, a retail bank with a large client base but a market capitalization of less than one billion USD, might be excluded due to this sample selection procedure. However, this threshold has been introduced for two reasons: First, publicly traded companies of this size often have more complex corporate structures with several subsidiaries and are more likely to suffer from a cyber risk incident. For example, Kamiya et al. (2021) identify a positive relationship between firm size and the probability of suffering from a cyberattack especially for financial firms by using data breaches from Privacy Rights Clearinghouse (PRC), the largest public US database (see also Ettredge

[10]We thereby make use of the sentiment word lists in Loughran and McDonald (2016), who propose the website Software Repository for Accounting and Finance (SRAF) of the University of Notre Dame, where the authors provide a spreadsheet of the sentiment word lists containing seven different sentiment categories (negative, positive, uncertainty, litigious, strong modal, weak modal and constraining). We use the update as of 2018, converting the original negative sentiment spreadsheet into a plain text document in lowercase and determine the absolute number of words in a similar way as the 1-gram extraction.

[11]In the treatment-effects model approach, Tobin's Q is used as a continuous and dependent variable (see also Bohnert, Fritzsche, et al., 2019). One disadvantage of using Tobin's Q as a function of CyberRM and other variables is the potential selectivity bias due to the endogeneity of the CyberRM choice. Therefore, the described maximum-likelihood treatment-effects model is used, as it allows for standard error adjustments through firm-level clustering (see Hoyt and Liebenberg, 2011; Petersen, 2009).

TABLE 3 Sampling procedure based on financial reporting as of December 31, 2018.

Screening criteria	Total market capitalization in USD (% of market capitalization)		Total number of firms	Number of US banks	Number of US insurers
Total number of US banks[a] and insurers with market capitalization in Thomson Reuters Eikon	2,864,049 million USD	100.00%	941	795	146
After exclusion of small-cap firms (<one billion USD market capitalization)	2,738,399 million USD	95.61%	203	129	74
After exclusion of firms without complete annual reports for the sample period 2011–2018[b]	2,605,372 million USD	90.97%	167	107	60
After exclusion of mid- or large-cap firms with an incomplete fiscal year	2,595,870 million USD	90.64%	163	103	60
After checking the availability of financial data for determinants from Thomson Reuters Eikon (see determinants in Section 2.3)	2,389,113 million USD	83.42%	137	97	40
After removing insurance brokers/advisors	2,273,125 million USD	78.40%	132	97	35
After removing nonfinancial conglomerates and firms with other business models[c]	1,704,266 million USD	59.51%	124	93	31

Note: The sample was extracted from Thomson Reuters Eikon at the beginning of 2019.

[a]In the subsequent analysis, the term "bank" is used for a bank (holding), a financial holding or a savings and loans holding, which conducts its activities through a bank (see also the Federal Financial Institutions Examination Council [FFIEC] for definitions of US institutions https://www.ffiec.gov/, accessed: 05/09/2021) and is categorized as a bank, according to TRBC sector classification.

[b]The exclusion also contains the merger between two firms during the sampling period.

[c]Mixed conglomerates are excluded which operate with subsidiaries extensively in nonfinancial services (i.e., which are commercially or industrially orientated). A major reduction in market capitalization for US insurers is based on the exclusion of Berkshire Hathaway Inc. with 502,600 million USD as a mixed conglomerate. Providers of risk management solutions or companies with other business models (except banks and insurers) are excluded, based on SEC annual reports and company descriptions from Thomson Reuters Eikon.

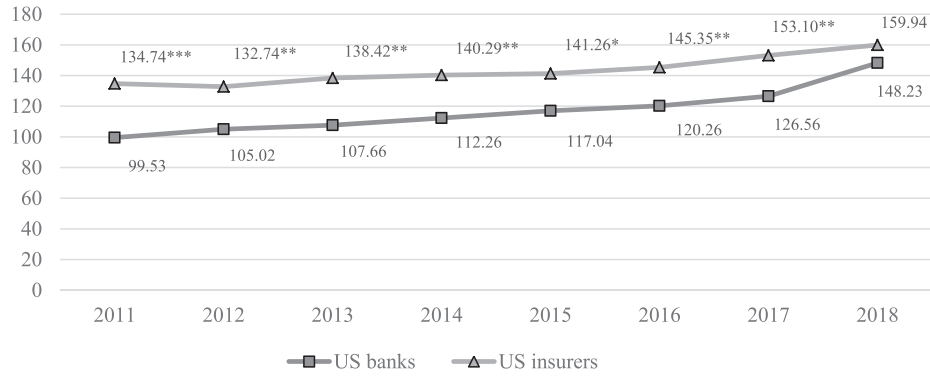

FIGURE 1 Development of mean cyber risk consciousness scores from 2011 to 2018, based on the annual reports of US banks and insurers. Differences between the mean cyber risk consciousness scores of US banks and insurers are examined using a two-sample *t* test. ***, **, * indicate the 1%, 5%, and 10% statistical significance level, respectively.

et al., 2018; Higgs et al., 2016 for further evidence).[12] Second, the inclusion of smaller firms with a market capitalization below one billion USD over multiple years (in our case $941 - 203 = 738$ small-cap firms over 8 years before exclusions) would not be feasible as in contrast to the generally easily available financial data, the text mining analysis would require all 5904 additional annual reports to be stored and converted for use in RapidMiner, with an additional manual review to determine whether CyberRM has been implemented.

We next exclude firms with incomplete annual reports over the sample period from 2011 to 2018. We use standardized annual reports on Form 10-K from the Electronic Data Gathering, Analysis and Retrieval (EDGAR) system of the US SEC. Finally, we exclude firms with short fiscal years, incomplete data for the determinants, insurance broker/advisors, nonfinancial conglomerates and firms with other business models from the data set, leading to a sample of 124 firms comprising 93 US banks and 31 US insurers (see Table A4 for the list of company names) and 992 firm-year observations overall. Over the considered time period, none of these undertakings became insolvent as a consequence of a cyber risk event and therefore, we can assume that there is no survivor bias.

3 | TEXTUAL AND EMPIRICAL RESULTS

3.1 | Firms' awareness of cyber risk

Figure 1 shows the development of our cyber risk consciousness score based on the text mining process and the statistical significance of the results, by applying a two-sample *t* test to differences in means between US banks and insurers. In general, we can see an increasing

[12]The one billion USD threshold for large- and mid-cap firms is also implemented by Corbet and Gurdgiev (2019), who examine systematic risk and contagion, caused by cyber events in the case of publicly traded corporations from 2005 to 2015. The authors argue that companies of this size have "significant linkages" to global financial markets and are more likely to cause contagion effects, which is supported by their evidence in relation to the contagion effects for all firms, and which in our case indicates a greater necessity to implement CyberRM.

awareness regarding cyber risks as reflected in an increasing mean score over the sample period from 2011 to 2018, which holds for both the banking and insurance industry. This is consistent with Berkman et al. (2018) who find a rising mean cybersecurity awareness score (for nonfinancial firms) from 2012 to 2016.

Moreover, Figure 1 shows that US insurers exhibit higher cyber risk consciousness scores over the entire sample period, which is in line with the fact that over a long time period, the US cyber insurance market has been the most developed worldwide (see Biener, Eling, & Wirfs, 2015) and that US property and casualty insurers report cyber risk as a material risk in their annual reports (see Pooser et al., 2018). Moreover, regulation seems to be a driver for an increasing cyber risk consciousness score, as annual reports emphasize the introduction of the Cybersecurity Bill of Rights for US insurers in 2015 by the National Association of Insurance Commissioners (NAIC), as well as the NAIC Insurance Data Security Model Law in 2017. Overall, cybersecurity disclosures became increasingly relevant for US companies against the background of the "CF Disclosure Guidance: Topic No. 2 and Issues of Cyber Disclosure" of the (Securities and Exchange Commission SEC, 2011, 2018) and the security breach notification laws (see Kamiya et al., 2021; National Conference of State Legislatures [NCSL], 2020), as also laid out in Section 2.2.

The mean cyber risk consciousness score of US banks is significantly lower as compared to US insurers throughout the sample period, except for 2018. In the case of US banks, relevant regulations which may have increased this score include the CISA of 2015 and the Enhanced Cyber Risk Management Standards from 2016 onwards.

The examination of the annual reports further shows that the NIST cybersecurity framework is considered highly relevant by US banks and insurers. In addition, certain US state-level regulations, in particular, e.g., the CCPA of 2018, the South Carolina Security Bill or the NYDES Cybersecurity Regulation from 2018 are mentioned in the reports (see also Section 2.2). Overall, in 2018 as the last year studied, we identify the highest mean cyber risk consciousness score for all observed firms, which is also consistent with the new 2018 regulations related to cyber risk in the US on Public Company Cybersecurity Disclosures, as laid out in Section 2.2. Furthermore, as mentioned in Section 2.3 and documented in Tables A4–A6, the majority of US banks and insurers in our sample are subject to a data breach notification law.

3.2 | US banks and insurers with a CyberRM implementation based on annual reports

The development of the number of firms that implemented CyberRM according to their annual reports from 2011 to 2018 is shown in Table 4. Following a manual assessment according to the procedure described in Table 2, we identify 626 firm-year observations (out of 124 firms × 8 years = 992 firm-year observations) with a CyberRM implementation (= 1a, 1b, or 1c). In particular, in 2018, 5 out of 124 companies took into account cyber risks in their OpRM, that is, CyberRM = 1a. Furthermore, we classified 91 firms in the category of CyberRM = 1b (based on criteria and keywords, no own risk category) and 6 firms had their own risk category (CyberRM = 1c) in their 2018 report.

TABLE 4 Number of firms with different levels of CyberRM (see Table 2 for a description of CyberRM levels; overall 124 firms × 8 years = 992 firm-year observations).

	CyberRM = 1a (integration into OpRM)		CyberRM = 1b (based on the criteria and keywords in Table A1, no own risk category)		CyberRM = 1c (own risk category)		
Year	US banks	US insurers	US banks	US insurers	US banks	US insurers	Firm-years
2011/before	0	0	36	8	1	0	45
2012	1	0	42	11	1	0	55
2013	3	1	45	12	2	0	63
2014	7	0	52	13	3	0	75
2015	8	0	64	15	3	0	90
2016	5	0	70	17	3	0	95
2017	6	0	74	17	3	1	101
2018	5	0	74	17	5	1	102
Σ	35	1	457	110	21	2	626

3.3 | Determinants of cyber risk management

3.3.1 | Univariate and bivariate results

Table 5 presents the descriptive summary statistics for all firm-year observations and provides first insights regarding the differences between means and medians.[13] The Pearson and Spearman correlation coefficients between CyberRM, determinants and Tobin's *Q* are reported in Table A7. We find a statistically positive relationship between CyberRM and the determinants *Size*, *Leverage, Bank*, *CyberRiskAwareness*, and *RiskAwareness*, a negative determinant for *RoA* and both a positive/negative determinant for *CapitalOpacity*.[14] Concerning *CyberRM* and *Q*, we observe a negative correlation.

Group differences in relation to the means and medians of firms with and without CyberRM are shown in Table 6. With respect to the value-relevance, we observe a Tobin's *Q* greater than 1 for the means and medians regardless of group affiliation. However, group differences in terms of means indicate that firms with CyberRM exhibit a lower mean and median with regard to Tobin's Q as compared to companies without CyberRM. We further observe that the determinants *Size*, *Leverage*, *Bank*, *CyberRiskAwareness*, and *RiskAwareness* are

[13]The cyber risk consciousness score shows a high standard deviation, indicating the occurrence of outliers, which is in line with the findings of Berkman et al. (2018) and does not lead to adjustments of the sample. The maximum of the cyber risk consciousness score is 1533 for only 1 firm-year observation (Key Corp in 2018). All other cyber risk consciousness scores are considerably less than 448 (second highest score).

[14]The absence of absolute correlation coefficients above a threshold value of 0.8 can be considered as an indication that multicollinearity does not pose a problem in our analysis (see Mason & Perreault, 1991). The computation of variance inflation factors (VIF) to additionally test for multicollinearity, confirms the results of the correlation analysis, as the VIFs are below the threshold value of 10 (see Marquardt, 1970).

TABLE 5 Summary statistics.

	Mean	Std. dev.	Min.	1st Quart.	Median	3rd Quart.	Max.
Q	1.0478	0.0830	0.8212	1.0024	1.0338	1.0740	1.7290
CyberRM	0.6310	0.4828	0.0000	0.0000	1.0000	1.0000	1.0000
Size	16.7360	1.5241	13.7289	15.6915	16.3438	17.2872	21.6874
Leverage	6.4884	5.1627	0.4368	4.0284	5.6552	7.2461	59.4598
RoA	0.0118	0.0095	−0.0151	0.0077	0.0100	0.0128	0.0802
CapitalOpacity	0.0299	0.0400	0.0003	0.0105	0.0223	0.0380	0.4916
Bank	0.7500	0.4332	0.0000	0.5000	1.0000	1.0000	1.0000
CyberRiskAwareness	123.6089	77.0989	4.0000	79.0000	107.0000	148.0000	1533.0000
RiskAwareness	0.3468	0.2245	0.0000	0.2704	0.3267	0.3989	6.5558
$Tone_{neg}$	7.2311	0.5878	1.9459	7.0031	7.1974	7.5224	8.6415

Note: Total number of firm-year observations is 992.

TABLE 6 Differences between groups with and without CyberRM.

	CyberRM = 1 (626 firm-year observations)		CyberRM = 0 (366 firm-year observations)		Differences	
	Mean	Median	Mean	Median	Differences in means	Differences in medians
Q	1.0390	1.0300	1.0628	1.0399	−0.0238***	−0.0099***
Size	16.9852	16.5538	16.3099	16.0575	0.6753***	0.4963***
Leverage	6.9615	5.7646	5.6793	5.2807	1.2822***	0.4839***
RoA	0.0102	0.0096	0.0145	0.0107	−0.0043***	−0.0011***
CapitalOpacity	0.0280	0.0232	0.0330	0.0207	−0.0050	0.0025**
Bank	0.8195	1.0000	0.6311	1.0000	0.1884***	0.0000***
CyberRiskAwareness	139.7652	124.0000	95.9754	84.5000	43.7898***	39.5000***
RiskAwareness	0.3766	0.3548	0.2958	0.2884	0.0808***	0.0664***
$Tone_{neg}$	7.2953	7.2399	7.1213	7.1577	0.1740***	0.0822***

Note: Differences in means are based on a two-sample *t* test; for differences in medians, a nonparametric Wilcoxon's rank-sum test is used.

***, ** indicate the 1% or 5% statistical significance level, respectively.

significantly higher in terms of mean and median for firms with CyberRM, and that firms with CyberRM tend to be less profitable (RoA) and more opaque.

We also report on the differences between US banks and insurers. Table 7 shows that US banks tend to have a higher general risk awareness. In terms of mean and median, significantly more US banks have adopted CyberRM than US insurers and have a significantly higher risk awareness, even though the cyber risk consciousness score is

TABLE 7 Differences between the US banking and insurance industry.

	US bank = 1 (744 firm-year observations)		US insurer (US bank = 0) (248 firm-year observations)		Differences	
	Mean	Median	Mean	Median	Differences in means	Differences in medians
Q	1.0385	1.0329	1.0756	1.0393	−0.0371***	−0.0064**
CyberRM	0.6895	1.0000	0.4556	0.0000	0.2339***	1.0000***
Size	16.6143	16.2821	17.1013	16.8097	−0.4870***	−0.5276***
Leverage	6.4532	5.9257	6.5941	3.0038	−0.1409	2.9219***
RoA	0.0095	0.0096	0.0187	0.0167	−0.0092***	−0.0071***
CapitalOpacity	0.0285	0.0244	0.0339	0.0116	−0.0054	0.0128***
CyberRiskAwareness	117.0685	101.0000	143.2298	121.0000	−26.1613***	−20.0000***
RiskAwareness	0.3609	0.3351	0.3054	0.2964	0.0555***	0.0387***
$Tone_{neg}$	7.0901	7.1265	7.6541	7.6131	−0.5640***	−0.4866***

Note: Differences in means are based on a two-sample *t* test; for differences in medians, a nonparametric Wilcoxon's rank-sum test is used.

***, ** indicate the 1% or 5% statistical significance level, respectively.

significantly higher for US insurers (among the reasons might be the word count involving cyber insurance products and relevant regulations, for instance). Concerning value variables, we also find that the (means and) medians for US banks are significantly higher with respect to *Leverage and CapitalOpacity* and significantly lower regarding *Tobin's Q*, *Size* and *RoA*. We therefore conduct the multivariate analyses regarding determinants and value separately for both industries.

3.3.2 | Multivariate results of the logistic regression model regarding the determinants of CyberRM

The results of the logistic regression regarding determinants of CyberRM for all financial firms in Table 8, Panel A, show that more profitable companies are less likely to adopt CyberRM, whereas firms associated with the banking industry, with a higher cyber risk consciousness score and greater risk awareness, are more likely to implement CyberRM.

Most of these results are in accordance with our hypotheses (see Section 2.3). With respect to *Size* (H1), *Leverage* (H2), and *CapitalOpacity* (H4), we do not find statistically significant relationships for the entire sample. The statistically significant negative result of *RoA* (H3) and *CyberRM* is in contrast to our hypothesis, suggesting that more profitable firms are less likely to implement CyberRM. Consistent with our hypothesis, we find evidence that banks (H5) are more likely to establish CyberRM with their higher exposure to spillover and systemic risk (see Eling & Pankoke, 2016; Heidinger & Gatzert, 2018), which may also result from cyber events that have occurred.

TABLE 8 Results of the logistic regression regarding the determinants of CyberRM.

Panel A. Logistic regression results regarding the CyberRM determinants of all firms				
R^2 = 0.2713	**Predicted relationship**	**Parameter estimate (β)**	**Standard error**	**Odds ratio (exp(β))**
Size	+	−0.0173	0.0721	0.9828
Leverage	+	0.0220	0.0251	1.0223
RoA	+	−29.4749**	11.9132	0.0000
CapitalOpacity	+	0.5144	2.6303	1.6726
Bank	+	1.3942***	0.2388	4.0318
CyberRiskAwareness	+	0.0159***	0.0022	1.0161
RiskAwareness	+	3.9935***	0.9514	54.2421

Panel B. Logistic regression results regarding CyberRM determinants of the US insurance and banking industry						
	US banks (R^2 = 0.2404)			**US insurers (R^2 = 0.3214)**		
	Parameter estimate (β)	**Standard error**	**Odds ratio (exp(β))**	**Parameter estimate (β)**	**Standard error**	**Odds ratio (exp(β))**
Size	−0.0162	0.0826	0.9840	−0.2907*	0.1720	0.7477
Leverage	−0.0032	0.0393	0.9968	0.0640	0.0455	1.0661
RoA	6.6603	26.0297	780.7849	−52.8306***	16.3114	0.0000
CapitalOpacity	4.8314	5.2053	125.3862	1.7996	3.6666	6.0472
CyberRiskAwareness	0.0174***	0.0029	1.0175	0.0160***	0.0043	1.0161
RiskAwareness	3.8013***	1.0998	44.7585	5.3597***	2.0523	212.6515

Note: The dependent variable is *CyberRM*. Panel A: Dummy variables are included to control for year-fixed effects. We also ran logistic regression with robust standard errors where the results remained unchanged and standard errors were adjusted for 124 firm-level clusters, when *RoA* became statistically insignificant. Panel B: Dummy variables are included to control for year-fixed effects. We also ran logistic regression with robust standard errors for US banks and insurers separately. The results remain unchanged (now RiskAwareness** for US insurers). The logistic regression with standard errors adjusted for 93 firm-level clusters based on US banks confirm the statistical significance for the variables *CyberRiskAwareness**** and *RiskAwareness***. The logistic regression with standard errors adjusted for 31 firm-level clusters based on US insurers confirm the statistical significance for the variables *RoA** and *CyberRiskAwareness**.

***, **, * indicate the 1%, 5% or 10% statistical significance level, respectively.

We also observe a significant positive relationship between *CyberRiskAwareness* (H6) and CyberRM, which is in line with Berkman et al. (2018). Furthermore, we replace the cyber risk consciousness score with the variable *Cyberattack*[15] as a proxy for cyber risk awareness, and find an insignificant positive relationship for all firm-year observations and US banks. Moreover, we run the logistic regression with *Cyberattack* as an additional indicator variable for a CyberRM implementation, and find a negative, but not statistically significant impact on CyberRM for all firms, as well as for US banks and insurers examined separately. Regarding general *RiskAwareness* (H7), we also find evidence of a significant positive impact on CyberRM, which is generally in line with Heidinger and Gatzert (2018)

[15]*Cyberattack* is set to 1 if a firm suffered from one or more cyberattacks in the firm-year investigated and 0 otherwise.

who observe an (insignificant) positive effect (in the context of reputation risk management).[16]

We also conducted separate logistic regressions for banks and insurers in Table 8, Panel B. In line with the results across all financial firms in Table 8, Panel A, we find a statistically significant positive impact of *CyberRiskAwareness* and *RiskAwareness* on CyberRM for both industries and (in the case of insurers) a significant negative effect of *RoA*. In contrast to our hypothesis, *Size* is significantly negative for insurers.

3.4 | The value of cyber risk management

3.4.1 | Results of the maximum-likelihood estimation of studying the value-relevance of CyberRM

We next study the impact of CyberRM on firm value. The adequacy of the simultaneous estimation concerning the *CyberRM* Equation (4) and the *Q* Equation (3) is assessed by conducting the likelihood-ratio test (to ensure the independence of the two equations) and the Wald test (goodness-of-fit) (see Bohnert, Gatzert, et al., 2019).[17]

As can be seen from Table 9, we find a positive and statistically significant relationship between *CyberRM* and *Tobin's Q*, which holds for all three samples, that is, for financial firms in the entire sample, as well as for banks and insurers separately, which confirms H_8. In particular, financial firms with CyberRM have a 10.92% higher firm value as compared to firms without CyberRM, when controlling for the endogeneity bias and relevant covariables. This positive effect seems to be particularly driven by insurance companies, who exhibit a 19.98% significant positive impact of CyberRM on Tobin's *Q*, compared to 6.37% in the case of banks. This finding is in line with Berkman et al. (2018) with regard to the value-relevance of cybersecurity awareness, and it is also consistent with most ERM research in relation to the positive impact of ERM on firm value (see Lechner & Gatzert, 2018; Pagach & Warr, 2011), especially regarding the insurance industry (see Bohnert, Gatzert, et al., 2019; Hoyt & Liebenberg, 2011).

Furthermore, the variable *Size* has a statistically significant negative effect on firm value for all three samples, whereas *RoA* exhibits a positive effect. The other variables depend on the sample (all

[16]We also ran the analysis including an indicator variable *state law* as a determinant for CyberRM, which is set to 1 if the respective state or jurisdiction of the incorporation or organization underlies an effective state security breach notification law. We find a significant negative relationship between *state law* and a CyberRM implementation. However, due to the small number of firm-year observations without *state law* and the concerns raised by Kamiya et al. (2021, p. 733) that "a firm's affected persons (for instance, customers) do not necessarily reside in its headquarters state, this result should be interpreted with caution," we do not include this variable in the logistic regression but conducted further analyses to gain more insight. We observe that the coefficient becomes insignificantly positive without year-fixed effects and that only including *state law* as the sole independent variable in the logistic regression results in an insignificant positive effect on CyberRM for US banks (and an insignificant positive Pearson correlation/Spearman's Rho between the two variables) and a negative one for US insurers. Removing the four US insurers from the sample that are not subject to the state security breach notification laws (see Table A6) also results in an insignificant positive Pearson correlation coefficient/Spearman's Rho for the entire sample and US banks. However, as mentioned above, one has to be cautious in the interpretation because of the small number of firm-year observations without *state law*.

[17]Both tests allow us to reject the Null hypothesis regarding the uncorrelatedness of residuals of the *CyberRM* Equation (4) and the *Q* Equation (3) at the 1% significance level (Wald test of independent equations instead of the likelihood-ratio test, due to the usage of robust standard errors) and the 1% significance level (second Wald test as a goodness-of-fit) (see Table 9).

TABLE 9 Results of the treatment-effects model regarding the impact of CyberRM on Tobin's *Q*.

	All firms		US banks		US insurers	
	***CyberRM* Equation (4)**	***Q Equation* (3)**	***CyberRM* Equation (4)**	***Q Equation* (3)**	***CyberRM* Equation (4)**	***Q Equation* (3)**
*CyberRM**		0.1092***		0.0637***		0.1998***
		(0.0130)		(0.0054)		(0.0263)
Size	0.1016***	−0.0158***	0.1813***	−0.0118***	0.0781	−0.0212***
	(0.0340)	(0.0021)	(0.0466)	(0.0012)	(0.0635)	(0.0072)
Leverage	−0.0646***		−0.2088***		-0.0322***	
	(0.0104)		(0.0342)		(0.0056)	
RoA	−48.8252***	4.0219***	−20.7956	3.9384***	−28.4950***	3.1461***
	(8.8053)	(0.7389)	(25.1772)	(0.7206)	(8.4136)	(0.9049)
CapitalOpacity	−4.1421**	0.3713***	−1.5453	−0.4096***	−3.8303*	0.6223***
	(1.9446)	(0.1314)	(2.6891)	(0.1049)	(2.2498)	(0.1201)
Bank		−0.0285***				
		(0.0079)				
CyberRiskAwareness	0.0056***		0.0084***		0.0085***	
	(0.0013)		(0.0019)		(0.0014)	
RiskAwareness	0.8419*		1.0617*		−0.4316	
	(0.4842)		(0.5428)		(0.7703)	
$Tone_{neg}$		−0.0304***		−0.0178***		−0.1097***
		(0.0049)		(0.0033)		(0.0192)
Constant	−1.2752**	1.4266***	−2.1993***	1.2914***	−1.7431*	2.1077***
	(0.5362)	(0.0468)	(0.8087)	(0.0270)	(0.9884)	(0.1747)
Observations		992		744		248
Wald test		181.93***		466.76***		170.56***
Wald test of indep. equations		53.41***		47.06***		41.47***

Note: The treatment-effects model is based on full maximum-likelihood estimation. *CyberRM** refers to the variable CyberRM with the endogenous treatment (see Bohnert, Gatzert, et al., 2019). Robust standard errors are given in parentheses. We also ran a treatment-effects model with standard errors adjusted for firm-level and firm-year clustering and the results remain unchanged. Furthermore, we ran the treatment-effects model and included the *Cyberattack* as an indicator variable in the *CyberRM* Equation (4). We found an insignificant negative relationship between *Cyberattack* and *CyberRM* for all firms and US insurers and an insignificant positive relationship in relation to US banks. The effect of *CyberRM* on *Tobin's Q* is 10.89%***, 6.39%*** and 19.94%*** for all firms, US banks and US insurers, respectively. Additionally, we ran the treatment-effects model by using *Cyberattack* as a proxy for *CyberRiskAwareness* in the *CyberRM* Equation (4) and observed an insignificant positive relationship between *Cyberattack* and *CyberRM* for all firms and US banks, as well as an insignificant negative relationship for US insurers. The effect of *CyberRM* on Tobin's Q is 11.75%***, 7.22%*** and 20.63%*** for all firms, US banks and US insurers, respectively.

***, **, * indicate the 1%, 5% or 10% statistical significance level, respectively.

firms, banks only, insurers only), including *CapitalOpacity* and *Bank*. With respect to $Tone_{neg}$, we find statistically significant effects on firm value for both banks and insurers separately, implying that a negative reporting tone can adversely affect firm value, in line with Berkmann et al. (2018).

3.4.2 | Robustness tests regarding the value-relevance of CyberRM

Robustness tests of the relationship between CyberRM and firm value for all firms are shown in Table A8 (*Q1–Q6*).[18] We thereby make adoptions of the *Q* Equation (3) and the *CyberRM* Equation (4) (*Q1–Q6*) by adding variables stepwise to examine the value-creation of a CyberRM implementation. The results of Wald tests thereby support the appropriateness of the maximum-likelihood treatment-effects approach in *Q1–Q6*.

We also study the impact of the different CyberRM levels as defined in Table 2 on firm value in Table A9. In line with the 10.92% benefit of CyberRM in terms of firm value in Table 9, with respect to the integration of cyber risk into OpRM only (CyberRM = 1a), we found a significant positive effect of 13.51% on firm value (only 35 firm-year observations for banks and one for insurers). The CyberRM identification based on criteria and keywords and requiring a framework, strategic guideline, committee/function, cyber risk mitigation or transfer measures as summarized in Table 2 (CyberRM = 1b, 457 firm-year observations for banks and 110 for insurers), shows a significant impact of 11.40% on firm value. Concerning cyber risks which are described under an own risk category in the risk management section with an established definition (CyberRM = 1c, 21 firm-year observations for banks and two for insurers), we found a significant positive effect of 12.57% on firm value. Overall, we thus found a significant positive impact of all CyberRM levels on firm value. However, in the case of CyberRM = 1a and 1c, in particular, the results should be interpreted with caution due to the lower number of firm-year observations.

With regard to the classification of firms to CyberRM level 0, 1a to 1c, we further checked the impact of different categorizations by also including (brief) statements regarding cyber/cybersecurity risk, information security risk or IT risk (e.g., a sentence in the "forward-looking statement and risk factors" section or in the OpRM section) in CyberRM level 1c. This resulted in 117 additional firm-year observations compared with the previous 23 firm-year observations in 1c, that is, 140 in total. In this case, we observed a comparable, significant positive effect of 10.71% on firm value (see Table A9).

Furthermore, we included *ERM* as an additional dummy variable in the *Q* Equation (3) based on the extended list of keywords proposed by Lechner and Gatzert (2018) and still found evidence of a statistically significant positive impact of CyberRM 10.46% on firm value (see Table A9).

Finally, we changed the dependent variable, Tobin's Q, and used *RoA* as an optional performance measure (see Bohnert, Gatzert, et al., 2019; Heidinger & Gatzert, 2018), which also showed a significant positive effect (0.91%) of CyberRM on RoA (see Table A9). This is generally not in line with the ERM literature, in which the RoA is highlighted as being "an accounting-based performance measure [which] incorporates large start-up and administrative costs of ERM activities"; this rather reflects negative effects, whereby Tobin's Q is more future-orientated (see, e.g., Bohnert, Gatzert, et al., 2019). The (slightly) positive effect observed suggests that the benefits of embedding CyberRM into ERM may outweigh the negative effects of costs.

[18]All robustness checks were also performed for US banks and insurers separately. In the notes of Table A8 and Table A9, we also report on the impact of CyberRM on Tobin's Q/RoA for US banks and insurers separately.

4 | SUMMARY

This paper examines the determinants and value of cyber risk management (CyberRM) in the US banking and insurance industry from 2011 to 2018 (124 large- and mid-cap firms). For this purpose, we first derive a cyber risk consciousness score using a text mining process, and second propose a list of keywords and phrases to identify different levels of CyberRM, based on 992 annual reports (Form 10-K). We then conduct a logistic regression to study the determinants of CyberRM and use a treatment-effects model to investigate the value-relevance of CyberRM.

Our results show that the awareness of cyber risks increased considerably in the US banking and insurance industry during the sample period, as reflected in increasing cyber risk consciousness scores, with regulation being one potential major driver. We also observe that US insurers have a higher cyber risk consciousness score than banks. At the same time, we identify a growing number of firms, which had implemented CyberRM, especially in the US banking sector.

Regarding CyberRM determinants, a logistic regression analysis shows that firms with a higher cyber risk consciousness and a higher risk awareness are more likely to adopt CyberRM, which also holds for both industries separately. By contrast with our assumption, the relationship between RoA and CyberRM was significantly negative, that is, profitable firms are less likely to implement CyberRM, which was the case for the entire sample and the insurer subsample. Consistent with our hypothesis, banks are more likely to implement CyberRM, which can be explained due to their greater exposure to spillover and systemic risk. We also found statistically significant evidence of a positive relationship between CyberRM and Tobin's *Q*, whereby firms with CyberRM have an 11% higher Tobin's *Q*, as compared to firms without CyberRM. Furthermore, robustness checks confirmed the significant positive relationship between CyberRM and firm value, both for each industry separately (6.37% for banks, 19.98% for insurers) and for different CyberRM levels.

Against a background of ongoing regulatory developments regarding cyber risks, we anticipate a further increasing awareness in the financial services industry, resulting in more and more banks and insurers implementing and improving CyberRM. Firms will have to establish a cyber risk strategy, a framework, a committee or function, as well as further cybersecurity measures, since cyber risk events can have a substantial, adverse effect on firms as shown by empirical event studies. Future research could extend the present work by specifically focusing on the situation of smaller firms.

ACKNOWLEDGMENTS

Madeline Schubert gratefully acknowledges the financial support from the Faculty Women's Prize, awarded by the Faculty of Business, Economics and Law at Friedrich-Alexander-Universität Erlangen-Nürnberg. The authors would like to thank two anonymous reviewers for helpful comments on an earlier version of the paper. We also appreciate valuable comments made by participants of the 4th World Risk and Insurance Economics Congress (08/2020), the Annual Meeting of the Western Risk and Insurance Association (03/2021) and the Annual Meeting of the German Insurance Association (03/2021). Open Access funding enabled and organized by Projekt DEAL.

CONFLICTS OF INTEREST

The authors declare no conflicts of interest.

DATA AVAILABILITY STATEMENT

Data available on request: The text mining data that support the findings of this study are available upon request from the corresponding author. Data subject to third party restrictions:

The financial data that support the findings of this study are available from Thomson Reuters Eikon (https://eikon.thomsonreuters.com/). Restrictions apply to the availability of these data, which were used under license for this study.

REFERENCES

Basel Committee on Banking Supervision (BCBS). (2018). Cyber-resilience: Range of practices. Retrieved November 26, 2019, from, www.bis.org

Baxter, R., Bedard, J. C., Hoitash, R., & Yezegel, A. (2013). Enterprise risk management program quality: Determinants, value relevance, and the financial crisis. *Contemporary Accounting Research*, *30*(4), 1264–1295.

Berkman, H., Jona, J., Lee, G., & Soderstrom, N. (2018). Cybersecurity awareness and market valuation. *Journal of Accounting and Public Policy*, *37*(6), 508–526.

Biener, C., Eling, M., Matt, A., & Wirfs, J. H. (2015). Cyber risk—Risikomanagement und Versicherbarkeit. *I-VW HSG Schriftenreihe*, 54.

Biener, C., Eling, M., & Wirfs, J. H. (2015). Insurability of cyber risk: An empirical analysis. *Geneva Papers on Risk and Insurance—Issues and Practice*, *40*(1), 131–158.

Bohnert, A., Fritzsche, A., & Gregor, S. (2019). Digital agendas in the insurance industry: The importance of comprehensive approaches. *Geneva Papers on Risk and Insurance—Issues and Practice*, *44*(1), 1–18.

Bohnert, A., Gatzert, N., Hoyt, R. E., & Lechner, P. (2019). The driver and value of enterprise risk management: Evidence from ERM ratings. *European Journal of Finance*, *25*(3), 234–255.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. *International Journal of Electronic Commerce*, *9*(1), 69–104.

Cebula, J. J., & Young, L. R. (2010). *A taxonomy of operational cyber security risks*. Software Engineering Institute, Carnegie Mellon University.

Corbet, S., & Gurdgiev, C. (2019). What the hack: Systemic risk contagion from cyber events. *International Review of Financial Analysis*, *65*, 1–18.

Cummins, J. D., Lewis, C. M., & Wei, R. (2006). The market value impact of operational loss events for US banks and insurers. *Journal of Banking & Finance*, *30*, 2605–2634.

Eling, M., McShane, M., & Nguyen, T. (2021). Cyber risk management: History and future research directions. *Risk Management and Insurance Review*, *24*(1), 1–33.

Eling, M., & Pankoke, D. A. (2016). Systemic risk in the insurance sector: A review and direction for future research. *Risk Management and Insurance Review*, *19*(2), 249–284.

Eling, M., & Schnell, W. (2016). What do we know about cyber risk and cyber risk insurance? *Journal of Risk Finance*, *17*(5), 474–491.

Ettredge, M. L., Guo, F., & Yijun, L. (2018). Trade secrets and cyber security breaches. *Journal of Accounting and Public Policy*, *37*, 564–585.

Fischer, E. A. (2014). *Federal laws relating to cybersecurity: Overview of major issues, current laws, and proposed legislations*. Retrieved September 30, 2019, from https://fas.org/sgp/crs/natsec/R42114.pdf

Froot, K. A., Scharfstein, D. S., & Stein, J. C. (1993). Risk management: Coordinating corporate investment and financing policies. *Journal of Finance*, *48*(5), 1629–1658.

Gatzlaff, K. M., & McCullough, K. A. (2010). The effect of data breaches on shareholder wealth. *Risk Management and Insurance Review*, *13*(1), 61–83.

Gordon, L. A., Loeb, M. P., & Sohail, T. (2010). Market value of voluntary disclosures concerning information security. *MIS Quarterly*, *34*(3), 567–594.

Heidinger, D., & Gatzert, N. (2018). Awareness, determinants and value of reputation risk management: Empirical evidence from the banking and insurance industry. *Journal of Banking & Finance*, *91*, 106–118.

Higgs, J. L., Pinsker, R. E., Smith, T. J., & Young, G. R. (2016). The relationship between board-level technology committees and reported security breaches. *Journal of Information Systems*, *30*(3), 79–98.

Hoyt, R. E., & Liebenberg, A. P. (2011). The value of enterprise risk management. *Journal of Risk and Insurance*, *78*(4), 795–822.

Kamiya, S., Kang, J.-K., Kim, J., Milidonis, A., & Stulz, R. M. (2021). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics*, *139*(3), 719–749.

Kessler, D. (2013). Why (re)insurance is not systemic. *Journal of Risk and Insurance*, *81*(3), 477–487.
Lechner, P., & Gatzert, N. (2018). Determinants and value of enterprise risk management: Empirical evidence from Germany. *European Journal of Finance*, *24*(10), 867–887.
Liebenberg, A. P., & Hoyt, R. E. (2003). The determinants of enterprise risk management: Evidence from the appointment of chief risk officers. *Risk Management and Insurance Review*, *6*(1), 37–52.
Loughran, T., & McDonald, B. (2016). Textual analysis in accounting and finance: A survey. *Journal of Accounting Research*, *54*(4), 1187–1230.
Maddala, G. S. (1983). *Limited-dependent and qualitative variables in econometrics*. Cambridge University Press.
Malhotra, A., & Kubowicz Malhotra, C. (2011). Evaluating customer information breaches as service failures: An event study approach. *Journal of Service Research*, *14*(1), 44–59.
Marotta, A., & McShane, M. (2018). Integrating a proactive technique into a holistic cyber risk management approach. *Risk Management and Insurance Review*, *21*(3), 435–452.
Marquardt, D. W. (1970). Generalized inverses, ridge regression, biased linear estimation, and nonlinear estimation. *Technometrics*, *12*(3), 591–612.
Mason, C. H., & Perreault, W. D. (1991). Collinearity, power, and interpretation of multiple regression analysis. *Journal of Marketing Research*, *28*(3), 268–280.
McShane, M., & Nguyen, T. (2020). Time-varying effects of cyberattacks on firm value. *Geneva Papers on Risk and Insurance—Issues and Practice*, *45*, 580–615.
Meulbroek, L. K. (2002). A senior manager's guide to integrated risk management. *Journal of Applied Corporate Finance*, *14*(4), 56–70.
National Conference of State Legislatures (NCSL). (2020). *Security breach notification laws*. Retrieved August 26, 2020, from www.ncsl.org
National Initiative for Cybersecurity Careers and Studies (NICCS). (2018). *A glossary of common cybersecurity terminology*. Retrieved September 30, 2019, from https://niccs.us-cert.gov/about-niccs/glossary
Nocco, B. W., & Stulz, R. M. (2006). Enterprise risk management: Theory and practice. *Journal of Applied Corporate Finance*, *18*(4), 8–20.
North, M. (2018). *Data mining for the masses with implementations in RapidMiner and R* (3rd ed.). Infinite Science, Lübeck.
Pagach, D., & Warr, R. (2011). The characteristics of firms that hire chief risk officers. *Journal of Risk and Insurance*, *78*(1), 185–211.
Petersen, M. A. (2009). Estimating standard errors in finance panel data sets: Comparing approaches. *Review of Financial Studies*, *22*(1), 435–480.
Pooser, D. M., Browne, M. J., & Arkhangelska, O. (2018). Growth in the perception of cyber risk: Evidence from U.S. P&C insurers. *Geneva Papers on Risk and Insurance—Issues and Practice*, *43*(2), 208–223.
Saunders, A., & Brynjolfsson, E. (2016). Valuing information technology related intangible assets. *MIS Quarterly*, *40*(1), 83–110.
Securities and Exchange Commission (SEC). (2011). *CF disclosure guidance: Topic No. 2: Cybersecurity*. Retrieved February 12, 2019, from www.sec.gov
Securities and Exchange Commission (SEC). (2018). *Commission statement and guidance on public company cybersecurity disclosures*. Retrieved January 20, 2020, from www.sec.gov
Shetty, S., McShane, M., Zhang, L., Kesan, J. P., Kamhoua, C. A., Kwiat, K., & Njilla, L. L. (2018). Reducing informational disadvantages to improve cyber risk management. *Geneva Papers on Risk and Insurance—Issues and Practice*, *43*(2), 224–238.
Xie, X., Lee, C., & Eling, M. (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.

How to cite this article: Gatzert, N., & Schubert, M. (2022). Cyber risk management in the US banking and insurance industry: A textual and empirical analysis of determinants and value. *Journal of Risk and Insurance*, 89, 725–763. https://doi.org/10.1111/jori.12381

APPENDIX A

Tables A1-A9.

TABLE A1 Criteria and keywords regarding the presence of framework/strategic guidelines, committee/function and cyber risk mitigation measures (at least one of the three criteria is satisfied).

I. Framework/strategic guidelines

- Action plans for cybercrime
- Corporate framework for cybersecurity
- Cyber and information security program
- Cyberattack plan
- Cyber control framework/program
- Cyber (resilience) program
- Cyber risk (management) framework/roadmap
- Cyber risk (reference/supervision) model
- Cybersecurity assessment framework
- Cybersecurity framework/guidance
- (Cyber)(security) incident response plan
- Cybersecurity (management) approach/program
- Cybersecurity policy/policies/(master)plan
- Cybersecurity risk management framework
- Cybersecurity risk management program
- Cybersecurity (risk mitigation) strategy
- Cyber threat management program
- NIST CSF (Cybersecurity Framework)
- Risk-based cybersecurity standard/process
- Information and technology risk management program
- Information security risk management program
- Information security and technology framework
- Information security framework/(master)plan
- Information security guidelines
- Information security policy/policies (and protocols) Information security program/policy
- Information security strategy/standards
- Information technology risk management policies
- Information technology risk management standards
- Information technology strategic plan
- ISO 27001 (ISO27002:2013, 27005, 13335:2004)
- IT risk (management) framework/principles
- IT risk security mechanism/strategy
- IT security policy/strategy and (master)plan/governance
- IT systems security strategy

Specific phrases of SEC Form 10-K disclosure

- Business continuity plan/program (addresses crisis management, business impact and data and systems recovery)
- Framework of controls, policies and technologies to monitor and protect information from cyberattacks, mishandling and loss, together with safeguards related to confidentiality, integrity and availability of information
- (Disaster recovery plan), policies and procedures (and service level agreements) designed to prevent or limit the effect/impact of systems failures, interruptions and security breaches (of information systems)/to protect the security and privacy of information
- Policies and procedures to identify, protect, detect, respond and recover from a possible security breach of its information systems and cyber-fraud

II. Committee/function/department

- Chief (Cyber and) Technology (Risk) Officer
- Chief Information Officer (CIO)
- Chief Information Security Officer (CISO)
- Computer security incident/(emergency) response team
- Control and prevention initiatives against cyberattack
- Cyber and IT controls
- Cyber (enterprise) board
- Cybersecurity information sharing and analysis networks
- Cybersecurity steering committee
- (Digital) security controls/division/operation center
- Innovation and/or technology committee
- Internal control system for cyber risk
- Security management (system focusing on cybersecurity risk)

(Continues)

- Cyber expertise response team
- Cyber resilience function
- Cyber risk committee
- Cyber solution group
- Cybercrime emergency/(expertise and) response team
- Cybercrime task force
- Cyber risk management firm
- Cybersecurity and fraud management
- Cybersecurity and technology control functions
- Cybersecurity and technology control organization
- Cybersecurity and technology control governance structure
- Cybersecurity collaboration networks
- Cybersecurity committee/subcommittee
- Cybersecurity experts/forum/officer/team
- Specialized units within the first line of defense dealing with cyber risk
- Center for information risk management
- (Corporate) information security division
- Information and cybersecurity department
- Information risk function/control structure
- Information security and resilience committee
- Information security department/team
- Information security oversight committee
- Information security risk (operating) committee
- Information technology risk management function
- IT security controls/department
- IT systems risk manager

III. Cyber risk mitigation and cyber risk transfer measures (at least two are fulfilled)

- Anti-cybercrime efforts/measures/initiatives
- Administrative and technical controls to prevent cyber incidents and protect information technology
- Cyberattack prevention
- Cyber (liability) insurance coverage/policy
- Cyber maturity assessment process
- Cyber risk protection projects
- Cybersecurity assessments/exercise/measures/updates
- Cybersecurity awareness program
- Cybersecurity controls
- Cybersecurity investments
- Cybersecurity monitoring and protection systems
- Cybersecurity practices/protocol
- Cybersecurity spending system
- Employee cybersecurity training
- Implementation of innovative cybersecurity solutions
- Improvement of resilience and (test) cybersecurity capabilities
- Investments in enhancing cyber defense capabilities
- Mandatory training in data and cybersecurity/customer education/campaigns for customers on spamming and phishing
- Mitigation plans for cybersecurity
- Program to increase employee awareness of cybersecurity risks and best practices
- Status report on cyber risk security

Specific phrases of SEC Form 10-K disclosure

- Controls to prevent, detect and appropriately react to such cyberattacks
- Cybersecurity and the continued development and enhancement of the controls and processes, designed to protect systems, computers, software, data and networks from attack, damage or unauthorized access
- Detection and response mechanisms, designed to contain and mitigate security incidents
- Defensive approach/measures/system (to manage the risk of a security breach or disruption/to implement safeguards)
- Integrity of systems through information security measures, risk management practices, relationships with threat intelligence providers and business continuity planning
- Monitor third party service providers' data and information security safeguards
- Physical, procedural and technological safeguards to prevent or limit the impact of system failures, interruptions and security breaches, and to protect confidential information from mishandling, misuse or loss
- Protective measures to maintain confidentiality, integrity and availability of information
- Update/upgrade systems and processes that are designed to protect the security of computer systems, software, networks and other technology assets

- Systems for cybersecurity protection, prevention and training - Information security (and privacy) training - Information security awareness program - Information security controls - Information security measures/procedures - Information security (annual) report - Information security safeguards - Internet security (and authentication) systems - IT fraud prevention - IT risk and IT security-related actions - IT risk assessments (and information security reports) - IT security measures - Security controls/measures	- Secure maintenance and transmission of confidential information - (Security and) integrity of (information) systems - Security and risk assessments on systems and those of third party service providers - Security measures and processes to defend against cybersecurity risks - Security systems to provide the security and authentication necessary to affect the secure transmission of data - Systems and processes that are designed to prevent security breaches - Technical controls/other preventive actions to reduce the risk of cyber incidents and protect our information technology

Note: In this table, we make adjustments regarding the uniform spelling of "cybersecurity" and "cyber risk," the standardized sequence of words, singular/plural forms and we remove the personal pronoun, "our," from certain phrases. The keywords of the three areas are listed alphabetically, with a focus on cyber(security), information security and IT risk. Additionally, we display separately certain phrases which are exclusively available in SEC Form 10-K reports.

TABLE A2 Extracts from the disclosures of firms' cyber (security) risk management systems.

SunTrust Banks (annual report 2018, pp. 58–59)—Excerpts from the manual identification of CyberRM (CyberRM = 1c: own risk category in the risk management section with an established definition of cyber/cybersecurity risk, IT risk or information security risk)	*Cybersecurity Risk Management* Our business activities and operations rely on our systems, computers, software, data, networks, the internet, and digital applications, as well as the systems and infrastructure of third parties. Our business, financial, accounting, data processing, or other systems or infrastructure may stop operating properly or become disabled or damaged as a result of a number of factors and influences that are wholly or partially beyond our control, such as potential failures, disruptions, or breakdowns, whether as a result of human error or intentional attack, as well as market conditions, fraudulent activities, natural disasters, electrical or telecommunications outages, political or social matters including terrorist acts, country risk, vendor risk, cyber-attacks, or other security risks. *The use of digital technologies introduces cybersecurity risk that can manifest in the form of information theft, criminal acts by individuals, groups, or nation states, or other disruptions to our Company's, clients', or third parties' business operations*. We use a wide array of techniques to secure our operations and proprietary information such as Board approved *policies and programs*, network monitoring, access controls, and dedicated security personnel, as well as consultation with third party data security experts. To control cybersecurity risk, we maintain an active *information security program* that is designed to

(Continues)

conform with FFIEC guidance. This *information security program* is designed to mitigate operational risks and is overseen by executive management, the Board, and our independent audit function. This program continually monitors and evaluates threats, events, and the performance of our business operations and continually adapts and modifies its risk mitigation activities accordingly. We also utilize appropriate *cybersecurity insurance* that controls against certain losses, expenses, and damages associated with cyber risk. In addition, our Board devotes significant time and attention to oversight of cybersecurity risk.

Further, we have adopted *the National Institute of Standards and Technology's Cybersecurity Framework* ("CSF") and perform periodic assessments against the framework to measure cybersecurity maturity. We also fully participate in the federally recognized financial sector information sharing organization structure, known as the Financial Services Information Sharing and Analysis Center. Digital technology is constantly evolving, and new and unforeseen threats and actions by others may disrupt operations or result in losses beyond our risk control thresholds. Although we invest substantial time and resources to manage and reduce cyber risk, it is not possible to completely eliminate this risk.

Our BRC reviews and approves *policies* relating to enterprise technology risk, *business continuity management, information security*, and enterprise data quality governance. The BRC also reviews and approves key technology risks and associated action plans. To ensure the integrity of our crisis management program, routine testing simulations are utilized to validate the viability of our plans. These ongoing tests are designed to provide assurance that our action plans are effective, valuable, and usable in the event of a significant business disruption. Crisis exercises are scenario-driven exercises that simulate impacts and consequences. Scenarios are developed through analysis of technology incidents, known cyber threats, internal stakeholder input, and industry trends.

We maintain an *information security education and awareness program* to provide consistent messaging to all users that may require access to our information about the need to maintain the security and privacy of that information. All users (i.e., full-time teammates, contractors, third parties, etc.) must complete this training before being granted access to our information systems. The content of the training

	program is reviewed annually to ensure that it addresses the current needs of our organization. In addition, communications to teammates through our intranet site, newsletters, email broadcasts, and targeted emails to select teammates, as necessary, foster awareness of information security risks. See Item 1A, "Risk Factors," in this Form 10-K for additional information regarding the risks associated with a failure or breach of our operational systems or infrastructure, including as a result of cyber-attacks.
Allstate Corporation (2018, p. 25) Excerpts from the manual identification of CyberRM (CyberRM = 1b: criteria and keywords in Table A1 are satisfied regarding the presence of framework/strategic guidelines, committee/function, or cyber risk mitigation/transfer measures)	Further, the New York State Department of Financial Services has issued cybersecurity regulations for financial services institutions, including banking and insurance entities, that impose a variety of detailed security measures on covered entities. The NAIC has also adopted the Insurance Data Security Model Law, which, if adopted as state legislation, would establish standards for data security and for the investigation of and notification to insurance commissioners of cybersecurity events. See the Regulation section, Privacy Regulation and Data Security, for additional information. Any failure or perceived failure by us to comply with such obligations may result in governmental enforcement actions and fines, litigation, or public statements against us by consumer advocacy groups or others, and could cause our employees and customers to lose trust in us, which could have an adverse effect on our reputation and business. Our *cyber and information security program* is continually enhanced to be resilient against emerging threats and improve our ability to detect and respond to attempts to gain unauthorized access to our data and systems. Cybersecurity system changes we implement that are designed to update and enhance our protective measures to address new threats may increase the risk of a system or process failure or the creation of a gap in our security measures due to the complexity and interconnectedness of our systems and processes. Any such failure or gap could adversely affect our business, reputation, results of operations or financial condition. From time to time, the Company and the Audit Committee engage independent advisors to assess and consult on cybersecurity matters. We also perform an on-going assessment of the quality of our program and identify opportunities to strengthen our *cybersecurity controls*. However, due to the increasing frequency and sophistication of such cyberattacks and changes in technology, there can be no assurance that a cyberattack will not take place with negative consequences, including an adverse effect to our business, results of operations and financial condition.

TABLE A3 Measurement and hypothesized sign of variables in regression models.

Variable	Measurement	Predicted sign[a]	References
CyberRM	1 = CyberRM (based on the three different CyberRM levels defined in Table 2), 0 = otherwise	+ (Tobin's *Q*)	N/A
Size	Natural logarithm of the book value of total assets	+ (CyberRM) +/− (Tobin's *Q*)	CMR (2004), NS (2006), GLS (2010), GM (2010), HL (2011), PW (2011), MKM (2011), BEW (2015), HPSY (2016), EGY (2018), LG (2018), PBA (2018), KKKMS (2021)
Leverage	Book value of liabilities/market value of equity	+ (CyberRM) +/− (Tobin's *Q*)	M (2002), HL (2011), PW (2011), BBHY (2013), HPSY (2016), PBA (2018), BGHL (2019), MN (2020), KKKMS (2021)
RoA	Firm's annual net income/book value of total assets	+ (CyberRM) + (Tobin's *Q*)	HL (2011), EGY (2018), PBA (2018), KKKMS (2021)
CapitalOpacity	Intangible assets/book value of total assets	+ (CyberRM) + (Tobin's *Q*)	CMR (2004), HL (2011), PW (2011), SB (2016), EGY (2018), LG (2018), KKKMS (2021)
Bank	1 = banking industry, 0 = insurance industry	+ (CyberRM)	K (2013), EP (2016), HG (2018), KKKMS (2021)
CyberRisk Awareness	Cyber risk consciousness score, based on text mining results	+ (CyberRM)	BJLS (2018)
CyberAttack	Alternative proxy for cyber risk awareness, 1 = observed firm which encountered a cyberattack, 0 = otherwise	+ (CyberRM)	BJLS (2018)
RiskAwareness	Term frequency of "risk" from text mining analysis compared with total number of words in annual reports, multiplied by 100	+ (CyberRM)	HG (2018)
Tobin's Q	(Market value of equity and book value of liabilities)/book value of assets	N/A	CMR (2004), GLS (2010), GM (2010), HL (2011), HG (2018), KKKMS (2021)
$Tone_{neg}$	Natural logarithm of negative terms of Loughran and McDonald's wordlist (updated version of 2018)	− (Tobin's *Q*)	LM (2016), BJLS (2018)

Note: References: M(2002): Meulbroek (2002); CMR(2004): Cavusoglu et al. (2004); NS(2006): Nocco and Stulz (2006); GLS (2010): Gordon et al. (2010); GM(2010): Gatzlaff and McCullough (2010); HL(2011): Hoyt and Liebenberg (2011); MKM(2011): Malhotra and Kubowicz Malhotra (2011); PW(2011): Pagach and Warr (2011); BBHY(2013): Baxter et al. (2013); K(2013): Kessler (2013); BEW(2015): Biener, Eling, & Wirfs (2015); EP(2016): Eling and Pankoke (2016); HPSY(2016): Higgs et al. (2016); LM(2016): Loughran and McDonald (2016); SB(2016): Saunders and Brynjolfsson (2016); BJLS(2018): Berkman et al. (2018); EGY(2018): Ettredge et al. (2018); HG(2018): Heidinger and Gatzert (2018); LG(2018): Lechner and Gatzert (2018); PBA(2018): Pooser et al. (2018); BGHL (2019): Bohnert, Gatzert, et al. (2019); MN (2020): McShane and Nguyen (2020); KKKMS(2021): Kamiya et al. (2021)

[a]Signs for Tobin's *Q* and CyberRM are indicated by the comments in brackets.

TABLE A4 Overview of the US banking and insurance industry sample with state or other jurisdiction of incorporation or organization from SEC annual reports (2011–2018).

US banking industry	
1st Source Corp (Indiana)	S&T Bancorp Inc. (Pennsylvania)
Ameris Bancorp (Georgia)	Sandy Spring Bancorp Inc. (Maryland)
Associated Banc-Corp (Wisconsin)	Seacoast Banking Corporation of Florida (Florida)
BancFirst Corp (Oklahoma)	Simmons First National Corp (Arkansas)
Bank of America Corp (Delaware)	South State Corp (South Carolina)
Bank of Hawaii Corp (Delaware)	Southside Bancshares Inc. (Texas)
BankUnited Inc. (Delaware)	SunTrust Banks Inc. (Georgia)
Banner Corp (Washington)	Synovus Financial Corp (Georgia)
Berkshire Hills Bancorp Inc. (Delaware)	TCF Financial Corp (Delaware)
BOK Financial Corp (Oklahoma)	Texas Capital Bancshares Inc. (Delaware)
Brookline Bancorp Inc. (Delaware)	Tompkins Financial Corp (New York)
Cathay General Bancorp (Delaware)	Trico Bancshares (California)
CenterState Bank Corp (Florida)	Trustmark Corp (Mississippi)
Chemical Financial Corp (Michigan)	U.S. Bancorp (Delaware)
CIT Group Inc. (Delaware)	UMB Financial Corp (Missouri)
Citigroup Inc. (Delaware)	Umpqua Holdings Corp (Oregon)
City Holding Co. (West Virginia)	Union Bankshares Corp (Virginia)
Columbia Banking System Inc. (Washington)	United Bankshares Inc. (West Virginia)
Commerce Bancshares Inc. (Missouri)	Valley National Bancorp (New Jersey)
Community Bank System Inc. (Delaware)	Webster Financial Corp (Delaware)
Cullen/Frost Bankers Inc. (Texas)	Wells Fargo & Co. (Delaware)
CVB Financial Corp (California)	WesBanco Inc. (West Virginia)
Eagle Bancorp Inc. (Maryland)	Westamerica Bancorp (California)
East West Bancorp Inc. (Delaware)	Western Alliance Bancorp (Nevada 2011–2013, Delaware)
F.N.B. Corp (Florida 2011-2015, Pennsylvania)	Wintrust Financial Corp (Illinois)
Fifth Third Bancorp (Ohio)	WSFS Financial Corp (Delaware)
First Bancorp (North Carolina)	Zions Bancorporation NA (Utah)
First Busey Corp (Nevada)	
First Citizens BancShares Inc. (Delaware)	*US insurance industry*
First Commonwealth Financial Corp (Pennsylvania)	Alleghany Corp (Delaware)
First Financial Bancorp (Ohio)	Allstate Corp (Delaware)
First Horizon National Corp (Tennessee)	American Financial Group Inc. (Laws of Ohio)
First Interstate BancSystem Inc. (Montana)	AXIS Capital Holdings Ltd. (Bermuda)

(Continues)

First Merchants Corp (Indiana)	Chubb Ltd. (Switzerland)
First Midwest Bancorp Inc. (Delaware)	CNA Financial Corp (Ohio)
Flagstar Bancorp Inc. (Michigan)	Employers Holdings Inc. (Nevada)
Fulton Financial Corp (Pennsylvania)	Enstar Group Ltd. (Bermuda)
Glacier Bancorp Inc. (Montana)	Fidelity National Financial Inc. (Delaware)
Hancock Whitney Corp (Mississippi)	First American Financial Corp (Delaware)
Heartland Financial USA Inc. (Delaware)	Genworth Financial Inc. (Delaware)
Heritage Financial Corp (Delaware)	Hanover Insurance Group Inc. (Delaware)
Hilltop Holdings Inc. (Maryland)	Hartford Financial Services Group Inc. (Delaware)
Home BancShares Inc. (Arkansas)	Horace Mann Educators Corp (Delaware)
Huntington Bancshares Inc. (Maryland)	Kemper Corp (Delaware)
Independent Bank Corp (Michigan)	Lincoln National Corp (Indiana)
International Bancshares Corp (Texas)	Markel Corp (Virginia)
JPMorgan Chase & Co. (Delaware)	Mercury General Corp (California)
KeyCorp (Ohio)	MetLife Inc. (Delaware)
Lakeland Financial Corp (Indiana)	Navigators Group Inc. (Delaware)
LegacyTexas Financial Group Inc. (Maryland)	Principal Financial Group Inc. (Delaware)
M&T Bank Corp (New York)	ProAssurance Corp (Delaware)
NBT Bancorp Inc. (Delaware)	Prudential Financial (New Jersey)
New York Community Bancorp Inc. (Delaware)	RenaissanceRe Holdings Ltd. (Bermuda)
Northwest Bancshares Inc. (Maryland)	Rli Corp (Illinois 2011-2017, Delaware)
Ocean First Financial Corp (Delaware)	Selective Insurance Group Inc. (New Jersey)
Old National Bancorp (Indiana)	Torchmark Corp (Delaware)
Pacific Premier Bancorp Inc. (Delaware)	Travelers Companies Inc. (Minnesota)
PacWest Bancorp (Delaware)	United Fire Group Inc. (Iowa)
Park National Corp (Ohio)	Unum Group (Delaware)
People's United Financial Inc. (Delaware)	W. R. Berkley Corp (Delaware)
Pinnacle Financial Partners Inc. (Tennessee)	
PNC Financial Services Group Inc. (Pennsylvania)	
Popular Inc. (Commonwealth of Puerto Rico)	
Prosperity Bancshares Inc. (Texas)	
Provident Financial Services Inc. (Delaware)	
Regions Financial Corp (Delaware)	

TABLE A5 Number of US banks/insurers with state security breach notification laws, according to state/jurisdiction from SEC annual reports 2011–2018 (see Kamiya et al., 2021; NCSL, 2020).

US state, effective date	Regulation (included in cyber risk consciousness score)	US banks	US insurers
Alabama, 06/01/2018	Ala. Code § 8-38-1 et seq.	0	0
Alaska, 07/01/2009	Alaska Stat. § 45.48.010 et seq.	0	0
Arizona, 12/31/2006	Ariz. Rev. Stat. § 18-545	0	0
Arkansas, 08/12/2005	Ark. Code §§ 4-110-101 et seq.	2	0
California, 07/01/2003	Cal. Civ. Code §§ 1798.29; 1798.82	3	1
Colorado, 09/01/2006	Colo. Rev. Stat. § 6-1-716	0	0
Connecticut, 01/01/2006	Conn. Gen Stat. §§ 36a-701b, 4e-70	0	0
Delaware, 06/28/2005	Del. Code tit. 6, § 12B-101 et seq.	29 (+1: 2014)	16 (+1: 2018)
District of Columbia, 07/01/2007	D.C. Code §§ 28-3851 et seq., 2020 B 215	0	0
Florida, 07/01/2014	Fla. Stat. §§ 501.171, 282.0041, 282.318(2)(i)	3 (−1: 2016)	0
Georgia, 05/05/2005	Ga. Code §§ 10-1-910, -911, -912; § 46-5-214	3	0
Guam, 07/11/2009	9 Guam Code Ann. (GCA) §§ 48.10 et seq.	0	0
Hawaii, 01/01/2007	Haw. Rev. Stat. § 487N-1 et seq.	0	0
Idaho, 01/01/2006	Idaho Stat. §§ 28-51-104 to -107	0	0
Illinois, 06/27/2006	815 ILCS §§ 530/1 to 530/25	1	1 (−1: 2018)
Indiana, 07/01/2006	Ind. Code §§ 4-1-11 et seq., 24-4.9 et seq.	4	1
Iowa, 07/01/2008	Iowa Code §§ 715C.1, 715C.2	0	1
Kansas, 01/01/2007	Kan. Stat. § 50-7a01 et seq.	0	0
Kentucky, 07/15/2014	Ky. Rev. Stat. (KRS) § 365.732; KRS §§ 61.931 to 61.934	0	0
Louisiana, 01/01/2006	La. Rev. Stat. §§ 51:3071 et. seq.	0	0
Maine, 01/31/2006	Me. Rev. Stat. tit. 10 § 1346 et seq.	0	0
Maryland, 01/01/2008	Md. Code Com. Law §§ 14-3501 et seq.; Md. State. Govt. Code §§ 10-1301 to -1308	6	0
Massachusetts, 10/31/2007	Mass. Gen. Laws § 93H-1 et seq.	0	0
Michigan, 07/02/2007	Mich. Comp. Laws §§ 445.63, 445.72	3	0
Minnesota, 01/01/2006	Minn. Stat. §§ 325E.61, 325E.64	0	1
Mississippi, 07/01/2011	Miss. Code § 75-24-29	2	0
Missouri, 08/28/2009	Mo. Rev. Stat. § 407.1500	2	0
Montana, 03/01/2006	Mont. Code §§ 2-6-1501 to -1503, 30-14-1701 et seq., 33-19-321	2	0
Nebraska, 07/14/2006	Neb. Rev. Stat. §§ 87-801 et seq.	0	0
Nevada, 01/01/2006	Nev. Rev. Stat. §§ 603A.010 et seq., 242.183	2 (−1: 2014)	1

(Continues)

TABLE A5 (Continued)

US state, effective date	Regulation (included in cyber risk consciousness score)	US banks	US insurers
New Hampshire, 01/01/2007	N.H. Rev. Stat. §§ 359-C:19, 359-C:20, 359-C:21	0	0
New Jersey, 01/01/2006	N.J. Stat. § 56:8-161, 163	1	2
New Mexico, 01/16/2017	2017 H.B. 15, Chap. 36	0	0
New York, 12/07/2005	N.Y. Gen. Bus. Law § 899-AA, N.Y. State Techn. Law 208	2	0
North Carolina, 12/01/2005	N.C. Gen. Stat. §§ 75-61, 75-65	1	0
North Dakota, 06/01/2005	N.D. Cent. Code §§ 51-30-01 et seq.	0	0
Ohio, 02/17/2006	Ohio Rev. Code §§ 1347.12; 1349.19, 1349.191, 1349.192	4	2
Oklahoma, 11/01/2008	Okla. Stat. §§ 74-3113.1, 24-161 to -166	2	0
Oregon, 10/01/2007	Oregon Rev. Stat. §§ 646A.600 to .628	1	0
Pennsylvania, 06/20/2006	73 Pa. Stat. §§ 2301 et seq.	4 (+1: 2016)	0
Puerto Rico, 01/05/2006	10 Laws of Puerto Rico §§ 4051 et seq.	1	0
Rhode Island, 03/01/2006	R.I. Gen Laws §§ 11-49.3-1 et seq.	0	0
South Carolina, 07/01/2009	S.C. Code. § 39-1-90	1	0
South Dakota, 07/01/2018	S.D. Cod. Laws §§ 20-40-20 to -46 (2018 S.B. 62)	0	0
Tennessee, 07/01/2005	Tenn. Code §§ 47-18-2107; 8-4-119	2	0
Texas, 04/01/2009	Tex. Bus. & Com. Code §§ 521.002, 521.053	4	0
Utah, 01/01/2007	Utah Code §§ 13-44-101 et seq.	1	0
Vermont, 08/12/2012	Vt. Stat. tit. 9 §§ 2430, 2435	0	0
Virgin Islands, 10/17/2005	V.I. Code tit. 14 §§ 2208, 2209	0	0
Virginia, 07/01/2008	Va. Code §§ 18.2-186.6; 32.1–127.1:05	1	1
Washington, 07/24/2005	Wash. Rev. Code §§ 19.255.010, 42.56.590	2	0
West Virginia, 06/06/2008	W.V. Code §§ 46A-2A-101 et seq.	3	0
Wisconsin, 03/31/2006	Wis. Stat. § 134.98	1	0
Wyoming, 07/01/2007	Wyo. Stat. §§ 40-12-501 et seq.	0	0
Other jurisdictions of US banks/insurers (Bermuda: 3; Switzerland: 1)		0	4
Number of observed firms (124)		93	31

TABLE A6 Number of US banks and insurers underlying state security breach notification laws, according to the reported state or jurisdiction of incorporation or organization in the SEC annual reports, as shown in Table A5 (from the 93 banks and 31 insurers in the sample).

Year of observation	US banks operating under state security breach notification laws	US insurers operating under state security breach notification laws
2011	90	27
2012	90	27
2013	90	27
2014	93	27
2015	93	27
2016	93	27
2017	93	27
2018	93	27

Note: Three US banks in our sample are located in Florida, where state security breach notification laws became effective in 2014. With respect to US insurers, the jurisdiction of incorporation or organization from the SEC annual report is located outside the United States (Bermuda for three insurers and Switzerland for one insurer) (see also Tables A4 and A5).

TABLE A7 Pearson's and Spearman's ρ correlation coefficients (992 firm-year observations).

		CyberRM	*Q*	*Size*	*Leverage*	*RoA*	*Capital Opacity*	*Bank*	*CyberRisk Awareness*	*Risk Awareness*	$Tone_{neg}$
CyberRM	Pearson	1									
	Spear. Rho	1									
Q	Pearson	−0.1387***	1								
	Spear. Rho	−0.0860***	1								
Size	Pearson	0.2139***	−0.2660***	1							
	Spear. Rho	0.2102***	−0.2992***	1							
Leverage	Pearson	0.1199***	−0.4741***	0.3901***	1						
	Spear. Rho	0.1454***	−0.7455***	0.2994***	1						
RoA	Pearson	−0.2162***	0.4883***	−0.1388***	−0.4361***	1					
	Spear. Rho	−0.1626***	0.4745***	−0.1093***	−0.6473***	1					
CapitalOpacity	Pearson	−0.0598*	0.3265***	-0.0222	−0.2054***	0.3543***	1				
	Spear. Rho	0.0746**	0.0491	0.0480	−0.1832***	0.0833***	1				
Bank	Pearson	0.2099***	−0.1935***	−0.1385***	−0.0118	−0.4161***	−0.0579*	1			
	Spear. Rho	0.2099***	−0.0679**	−0.1311***	0.3152***	−0.2594***	0.2345***	1			
CyberRisk Awareness	Pearson	0.2742***	−0.1816***	0.5171***	0.2756***	−0.0654**	−0.0720**	−0.1470***	1		
	Spear. Rho	0.3725***	−0.2512***	0.5224***	0.1664***	−0.1064***	−0.0237	−0.2052***	1		
RiskAwareness	Pearson	0.1738***	−0.0902***	0.1650***	0.0634**	−0.0789**	−0.0677**	0.1065***	0.1773***	1	
	Spear. Rho	0.3624***	−0.1793***	0.3570***	0.2267***	−0.1297***	−0.0490	0.1972***	0.3971***	1	
$Tone_{neg}$	Pearson	0.1429***	−0.1409***	0.2945***	0.2375***	0.0112	−0.0311	−0.4157***	0.5467***	0.0718**	1
	Spear. Rho	0.1283***	−0.2592***	0.4171***	0.0498	−0.0594*	−0.0760**	−0.4751***	0.7307***	0.0966***	1

Note: 992 firm year observations.

***, **, * denotes statistical significance at 1%, 5%, or 10% level.

TABLE A8 Sensitivity analysis of the treatment-effects model

Variable	Q1	Q2	Q3	Q4	Q5	Q6
CyberRM	0.0016	−0.0261*	0.1216***	0.1230***	0.1124***	0.1092***
	(0.0056)	(0.0147)	(0.0108)	(0.0101)	(0.0116)	(0.0130)
Size	−0.0105***	−0.0087***	−0.0177***	−0.0179***	−0.0159***	−0.0158***
	(0.0013)	(0.0018)	(0.0020)	(0.0020)	(0.0020)	(0.0021)
RoA	3.0372***	2.9664***	4.4103***	4.2228***	4.1128***	4.0219***
	(0.5843)	(0.5990)	(0.7645)	(0.7469)	(0.7362)	(0.7389)
CapitalOpacity	0.3918***	0.3915***	0.2351*	0.3722***	0.3676***	0.3713***
	(0.1137)	(0.1138)	(0.1406)	(0.1355)	(0.1327)	(0.1314)
Bank	−0.0252***	−0.02542***	−0.0232***	−0.0229***	−0.0258***	−0.0285***
	(0.0075)	(0.0075)	(0.0077)	(0.0077)	(0.0079)	(0.0079)
$Tone_{Neg}$	−0.0199***	−0.0198***	−0.0172***	−0.0171***	−0.0305***	−0.0304***
	(0.0039)	(0.0039)	(0.0038)	(0.0036)	(0.0052)	(0.0049)
Constant	1.3370***	1.3250***	1.3505***	1.3493***	1.4226***	1.4266***
	(0.0394)	(0.0409)	(0.0428)	(0.0423)	(0.0483)	(0.0468)
CyberRM						
Size	0.2029***	0.1707***	0.2031***	0.2060***	0.1078***	0.1016***
	(0.0311)	(0.0369)	(0.0270)	(0.0272)	(0.0337)	(0.0340)
Leverage		0.0311	−0.0516***	−0.0544***	−0.0655***	−0.0646***
		(0.0198)	(0.0083)	(0.0087)	(0.0103)	(0.0104)
RoA			−48.5203***	−45.2540***	−49.5394***	−48.8252***
			(7.7018)	(8.0220)	(8.6381)	(8.8053)
CapitalOpacity				−4.8272*	−4.7157**	−4.1421**
				(1.9340)	(1.9672)	(1.9446)
CyberRiskAwareness					0.0059***	0.0056***
					(0.0013)	(0.0013)
RiskAwareness						0.8419*
						(0.4842)
Constant	−3.0412***	−2.7066***	−2.2533***	−2.1969***	−1.1132**	−1.2752**
	(0.5164)	(0.5590)	(0.4517)	(0.4506)	(0.5232)	(0.5362)
Number of observations	992	992	992	992	992	992

(Continues)

TABLE A8 (Continued)

CyberRM						
Wald-test	226.20***	212.57***	202.68***	216.69***	195.10***	181.93***
Wald-test of indep. equations	5.39**	4.80**	91.49***	112.67***	72.04***	53.41***

Note: The treatment-effects model is based on full maximum-likelihood estimation. Robust standard errors are given in parentheses. We also ran a treatment-effects model, with standard error adjusted, for 124 firm-levels, as well as firm-year clustering (8 firm-years) and the results remain unchanged. We conducted a sensitivity analysis for the *CyberRM Equation* for banks and insurers separately and reported on the impact of *CyberRM* on *Tobin's Q* in a stepwise manner, including the five variables (*Size, Leverage, RoA, CapitalOpacity, CyberRiskAwareness* and *RiskAwareness*) in the *CyberRM Equation* (US banks: 0.0122**, 0.0752***; 0.0741***, 0.0741***, 0.0648***, 0.0637***; US insurers: 0.2031***, −0.0373**, 0.2063***, 0.2116***, 0.1971***, 0.1998***). Moreover, we ran the treatment-effects model in a stepwise manner, including the five/four variables (*Size, RoA, CapitalOpacity, Bank, Tone*$_{neg}$) in the *Q* Equation for all firms, banks and insurers separately. We additionally reported on the effect of *CyberRM* on *Tobin's Q* (all firms: −0.0869***, 0.0047, −0.0006, 0.0009, 0.1092***; US banks: 0.0737***, 0.0633***, 0.0637***, 0.0637***; US insurers: −0.1047***, −0.0015, 0.1857***, 0.1998***).

***, **, * indicate the 1%, 5%, or 10% statistical significance level, respectively.

TABLE A9 Further robustness tests of the treatment-effects model.

Variables	**Q1**	**Q2**	**Q3**	**Q4**	**Q5**	**RoA**
CyberRM	0.1351***	0.1140***	0.1257***	0.1071***	0.1046***	0.0091***
	(0.0123)	(0.0101)	(0.0174)	(0.0087)	(0.0133)	(0.0008)
Size	−0.0095***	−0.0162***	−0.0109***	−0.0138***	−0.0168***	−0.0015***
	(0.0013)	(0.0020)	(0.0014)	(0.0017)	(0.0021)	(0.0002)
RoA	3.3093***	3.9556***	3.1402***	3.6689***	3.9743***	
	(0.5985)	(0.7218)	(0.5901)	(0.6240)	(0.7328)	
CapitalOpacity	0.4083***	0.3440**	0.3918***	0.3341***	0.3744***	0.0817***
	(0.1111)	(0.1374)	(0.1138)	(0.1263)	(0.1304)	(0.0118)
Bank	−0.0148**	−0.0269***	−0.0190***	−0.0079	−0.0285***	−0.0107***
	(0.0072)	(0.0078)	(0.0073)	(0.0069)	(0.0078)	(0.0009)
LNToneNeg	−0.0153***	−0.0287***	−0.0192***	−0.0157***	−0.0310***	−0.0033***
	(0.0037)	(0.0051)	(0.0037)	(0.0033)	(0.0048)	(0.0005)
ERM					0.0156***	
					(0.0058)	
Constant	1.2722***	1.4252***	1.3324***	1.3292***	1.4387***	0.0603***
	(0.0373)	(0.0475)	(0.0395)	(0.0406)	(0.0463)	(0.0050)
	CyberRM1a	***CyberRM1b***	***CyberRM1c***	***CyberRM1c all definitions***	***CyberRM***	***CyberRM***
Size	0.0657	0.1211***	0.1113***	0.1756***	0.0977***	0.0641*
	(0.0424)	(0.0310)	(0.0427)	(0.0265)	(0.0339)	(0.0361)

TABLE A9 (Continued)

	CyberRM1a	*CyberRM1b*	*CyberRM1c*	*CyberRM1c all definitions*	*CyberRM*	*CyberRM*
Leverage	−0.0721**	−0.0651***	−0.0292**	−0.0462***	−0.0629***	−0.0585***
	(0.0309)	(0.0104)	(0.0116)	(0.0120)	(0.0102)	(0.0084)
RoA	−41.1510***	−44.4464***	−30.549***	−40.9769***	−48.251***	
	(11.8091)	(8.3435)	(7.3292)	(7.0718)	(8.7987)	
CapitalOpacity	−14.869***	−4.0868**	−9.1417***	−6.0835***	−3.9301**	−3.7969**
	(2.7966)	(1.9523)	(2.9517)	(2.1719)	(1.9379)	(1.2598)
ScoreNew	−0.0058***	0.0044***	0.0008*	0.0002	0.0056***	0.0079***
	(0.0017)	(0.0010)	(0.0004)	(0.0003)	(0.0013)	(0.0012)
RiskAwareness	0.1818**	0.0666	0.1784**	0.0549	0.7854	2.1467***
	(0.0846)	(0.1996)	(0.0808)	(0.0582)	(0.4887)	(0.5217)
Constant	−0.8558	−1.4312**	−3.0114***	−2.9946***	−1.2121**	−1.9186***
	(0.8958)	(0.4854)	(0.7839)	(0.4807)	(0.5263)	(0.5436)
Number of observations	992	992	992	992	992	992
Wald-test	244.93***	217.47***	199.87***	230.95***	189.96***	249.61***
Wald-test of indep. equations	78.84***	99.86***	60.88***	144.05***	50.53***	75.06***

Note: The treatment-effects model is based on the full maximum-likelihood estimation. Robust standard errors are given in parentheses. We also ran the treatment-effects model, with standard error adjusted for 124 firm-levels, as well as firm-year clustering (8 firm-years) and the main results remain unchanged. We conducted robustness tests for banks and insurers separately and reported on the results (for the cases *Q2*, *Q5* and *RoA* when the separate computation of the treatment-effects model was appropriate, due to the small number of firm-year observations for all other cases). In relation to *Q2*, we found a significant positive impact of CyberRM = 1b on *Tobin's Q* (0.0694*** for banks; 0.2002*** for insurers). For *Q5*, we also found a significant positive impact of *CyberRM* on *Tobin's Q* (0.0612*** for banks; 0.1932*** for insurers). In the case of *RoA*, we observed a significant positive effect of *CyberRM* on *RoA* (0.0048*** for banks; 0.0112*** for insurers).

***, **, * indicate the 1%, 5% or 10% statistical significance level, respectively.