7-8-2023

The Impact of Competitive Threats from the Product Market on Data Breaches

Qiang CAO
City University of Hong Kong, qiangcao2-c@my.cityu.edu.hk

Xian Cheng
Sichuan University, beyoungbelong@gmail.com

Stephen Shaoyi LIAO
City University of Hong Kong, issliao@cityu.edu.hk

The Impact of Competitive Threats from the Product Market on Data Breaches

Short Paper

Qiang CAO
City University of Hong Kong
Hong Kong, China
qiangcao2-c@my.cityu.edu.hk

Xian CHENG
Sichuan University
Chengdu, China
chengcx@scu.edu.cn

Shaoyi Stephen LIAO
City University of Hong Kong
Hong Kong, China
issliao@cityu.edu.hk

Abstract

In this digital era, the concern about data breaches is rapidly increasing among consumers and firms. When the firm is facing competitive threats from the product market, would it perform well in data protection? Does the presence of a CIO/CTO help prevent a data breach? Would the impact of competitive threats on data breach vary by the severity of the data breach? In this study, by examining a sample of data breaches from 2005 to 2018, we find that competitive threats from the product market are positively associated with the likelihood of data breaches. And the presence of a CIO/CTO will also increase the likelihood of a data breach. It's somewhat different from prior studies. We plan to further explore the competitive threats' impact on different types of data breaches as well as their latent mechanism. Our study contributes a lot to IS cybersecurity and management literature.

Keywords: Cybersecurity, Data Breach, Competitive Threats

Introduction

The number of data breaches in the United States has increased sharply within the past 13 years from a mere 157 in 2005 to 1,257 by 2018. In the meantime, the number of data exposures increased from 66.9 million to 471.23 million.[1] The financial loss of a data breach is very large. Resolving a data breach takes U.S. firms 46 days, $21,155 per day on average (Haislip et al. 2021). Besides, both firms' market value and consumers' trust will also be damaged heavily (Goode et al. 2017; Janakiraman et al. 2018).

Given the important impact of the data breach, researchers are interested in identifying factors that could affect the likelihood of a data breach in a firm. Some work has pointed out that a firm's features, such as age, size, and cybercrime regulations would affect the likelihood of data breach (Cheng et al. 2017; McLeod and Dolezel 2018; Min Wang and Zuosu Jiang 2017). Previous literature in information systems (IS) research focuses on the impact of information technology (IT) infrastructure investment and firm governance (Angst et al. 2017; Haislip et al. 2021). However, very little research pays attention to the market

[1] https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/

factors' effect on the data breach.

Therefore, we aim to identify the association between a firm's competitive threats from the product market and the likelihood of a data breach. Competitive threats from the product market refer to the competition between a firm's products and its competitors' products (Li and Zhan 2019). When a firm's products are closer to its competitors, it will face a greater competitive threat. Since most data breaches originate from external threats [2], a firm's competitive threats from the product market could also have an impact on the data breach. On the one hand, firms that have a large set of products (they are facing large competitive pressure from the product market) usually face a great challenge in product data management. It is more vulnerable to hacking or data stealing. On the other hand, some firms would like to develop similar products to frustrate their competitor, which makes them attract more attacks from other rivals. Besides, since competitive threats could aggravate managerial career concerns (Li and Zhan 2019), it would affect the operation and management of the firm significantly. The weaknesses of firm governance would also attract more external attacks as well as internal stealing.

Besides, we also take the IT governance of the firm into our model. The moderating effect of IT governance on competitive threats from the product market on data breaches is unclear. Some research found that the presence of a CIO could reduce the risk of a data breach when the firm has a CEO/CFO with IT expertise (Haislip et al. 2021). However, other literatures found the presence of a CIO or board-level IT committee could not reduce the data breach risk. Instead, it would increase the likelihood of a data breach. Therefore, we would like to examine the impact of IT governance (presence of a CIO/CTO) in this study. What's more, we further examine the impact of competitive threats on different severity levels of data breaches.

Using data from 2005 to 2018, we find that firm with large competitive threats from the product market increases the likelihood of data breach. And the presence of the CIO/CTO could strengthen the likelihood of a data breach. We also find that competitive threats are more likely to increase the risk of severe data breaches but less likely to increase the risk of mild data breaches. Further studies, such as competitive threats' impact on different types of data breaches, and causal inference, are needed in the future.

Literature Review

Data Breach

A data breach is "a security violation in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an unauthorized individual" (Privacy Rights Clearinghouse 2019). A data breach could be a result of hacking, theft, lost, or mishandled.

There are four themes of data breach research. The first theme is the factors that result in the data breach. Firm governance, such as the IT expertise of the CEO and CFO (Haislip et al. 2021), the presence of a CIO (Smith et al. 2021), as well as the establishment of an IT-related committee (Higgs et al. 2016), are interest of many IS researchers. Besides, the wide range of environmental and organizational factors, such as firm social performance (D'Arcy et al. 2020), IT strategy, and security investment (Li et al. 2021; Liu et al. 2020), are also taken into account by some studies. The second theme is the impact of the data breach. Some research focuses on the impact on a firm's reputation (Gwebu et al. 2018), stock return(Lending et al. 2018), and firms' or consumers' behavior after the data breach (Ashraf 2022; Janakiraman et al. 2018). The third theme is related to the detection or prevention of data breaches using advanced techniques (Kumari et al. 2021; Rahulamathavan et al. 2015; Wang et al. 2004). The fourth theme is about the law of data protection and data breach notification (Bisogni and Asghari 2020; Schwartz and Janger 2007).

We could find most research in IS field focus on the factors that lead to data breach of firms. And most of them focus on IT governance. A wider range of environmental, and organizational factors are not fully explored. In this study, we aim to examine the impact of a firm's competitive threats from the product

[2] https://www.securitymagazine.com/articles/97089-us-data-breach-volume-increased-10-in-2021

market on the likelihood of data breaches as well as the impact of IT governance (the presence of a CIO or CTO).

Competitive Threats from the Product Market

Two streams study competitive threats from the product market. The first one is competitive threats' impact on firm performance, such as the relationship between competition pressure and stock crash (Li and Zhan 2019), competitive threats' impact on a firm's payout policy and cash holdings (Hoberg et al. 2014), as well as the innovation (Barbos 2015). The second stream mainly talks about a firm's reaction to competitive threats from the product market. Some firms would take action actively, such as increasing R&D (Research & Development) investment (Boubaker et al. 2022) and encouraging innovation (Chen et al. 2021). However, there is also some dark side to competitive threats. Some firms would be driven by short-interest pressure(Hughes-Morgan and Ferrier 2017), engage in corruption activities (Iriyama et al. 2016), drop-in employment investment (Autor 2003), and some other corporate crimes (Baumann and Friehe 2016).

Since most research about competitive threats from the product-market focus on the impact and firm reaction to competition pressure, the relationship between competitive threats and the cybersecurity of the firm (data breach in this context) has not been explored. In this study, we would like to examine the impact of a firm's competitive threats from the product market on the likelihood of data breaches as well as the impact of IT governance (the presence of a CIO or CTO). What's more, we further explore the impact of competitive threats on different severity levels of data breaches.

Hypotheses Development

Competitive Threats from Product Market's Impact on Firm's Data Breach

Competitive threats from the product market are not always good for firms. The main concerns about the impact of competitive threats on the risk of the data breach are 1) Developing more products to corner a competitive market is a typical strategy of some firms. Some of them even develop similar products to frustrate their competitor. However, the internal data management of so many products is a great challenge. Hackers are more likely to attack them. 2) firms with large competitive threats usually have more product similarities with their competitors. Their external rivals are more likely to attack them. Besides, more competitive threats would increase the prevalence of crime (Baumann and Friehe 2016), and corruption activities (Iriyama et al. 2016). Hiring hackers or internal employees to do damage to rivals' operations, such as hacking the database, or stealing files, is potential dirty work. Besides, the short-interest pressure could also enforce the firm focus on stock return (Li and Zhan 2019), HR training (Iriyama et al. 2016), or some other short-term investment. And then, the long-term investment, such as R&D investment (Boubaker et al. 2022; Li et al. 2021), data protection would be neglected. This could increase the risk of a data breach. What's more, competitive threats could distort the efficiency of firm employment decisions by reducing labor investment (Boubaker et al. 2022). Reducing the salary or welfare of employees would impair their activeness and productivity. It could increase the internal data breach risk. Therefore, we propose the following hypothesis:

H1 Competitive threats from the product market are positively related to a firm's data breaches.

Method

Data & Variables

We use Breach as the dependent variable. The data breach dataset is downloaded from the Privacy Rights Clearinghouse[3], a not-for-profit organization. It collects data breach events data from state government reporting agencies and various media outlets. This dataset represents mandatory disclosure of data breaches if customer records are lost. It has been used in several related studies (Haislip et al. 2021; Liu et al. 2020; Smith et al. 2021). We use *prodmktfluid* as the independent variable to measure competitive

[3] https://privacyrights.org/data-breaches

threats from the product market. It is developed by (Hoberg et al. 2014). This variable captures the similarity between a firm's products and the changes in its competitors' products in the product market. Since private firms and government entities have no publicly available financial data, we eliminate them. A larger *prodmktfluid* means the firm has more product overlap with its rival. That indicates a larger competitive threat. We also collected several control variables from Compustat, Audit Analytics, and BoardEx. We first include measures of size (emp, sale, at) and performance (leverage, xi, and mkvalt), because larger and more successful firms are more likely to be the targets of data breaches (Higgs et al. 2016; Wang et al. 2013). We then include include weakness-related variables (material_weakness, count_weak) found by audits because firms with weak internal control environments are more vulnerable to data breaches (Ashraf 2022; Bisogni and Asghari 2020). Besides, the IT governance of the firm is also included into control variables (CIO_CTO). Because some researchers have reported that the CIO/CTO may help reduce the data breach risk (Haislip et al. 2021). But another study found the firm with a CIO/CTO may be more likely to have data breach (Smith et al. 2021).

To reduce the skewness of our variables, we use their log transformation in our models.

After merging with data breach data, we have 38,791 observations (412 data breach events are left). Table 1 gives the introduction of variables.

Variables	Definition	Obs	Mean	Std. dev.	Min	Max
Breach	an indicator variable of a data breach, 1 if the firm reports a data breach in the current year, and 0 otherwise.	38,791	0.011	0.104	0	1
prodmktfluid	a variable measures competitive threats from the product market	38,791	7.127	3.752	0.063	24.609
CIO_CTO	an indicator variable of CIO/CTO presence, 1 if the firm reports the CIO/CTO position in the year and 0 otherwise	38,791	0.362	0.481	0	1
emp	Employees	38,791	10.766	51.650	0	2300
sale	Gross sales	38,791	3527.305	15328.17	-4234.472	496785
leverage	total liabilities divided by total assets in year t	38,700	0.591	0.674	0	62.721
mkvalt	market value - total	36,734	5212.152	23948.62	0.058	1073391
at	assets – total	38,791	6.792	2.097	0.000	14.986
material_weakness	material weakness	38,790	0.255	0.945	0	12
count_weak	count of internal control weak	38,791	0.274	1.606	0	72
xi	extraordinary items	38,791	8.212	0.042	0.000	8.360

Table 1 Variable Descriptions

Model Specifications

To test our hypothesis about the association between competitive threats from the product market on data breaches, we specify the following Logit and Poisson regression with time-fixed effects:

$$Breach_{it} = \beta_0 + \beta_1 ln\_prodmktfluid_{it} + \beta_2 X_{it} + B_t + \varepsilon_{it} \quad (1)$$

where Breach equals one if the firm reports a data breach in the current year t and zero otherwise. X_{ct} represents the control variables. B_t is the time-fixed effect, respectively.

Since the likelihood of a data breach occurring is low, there are many zero values in our dependent variable. Therefore, we also employ the zero-inflated model (zero-inflated Poisson regression) in our study. The inflate factor in this model is whether the audit report shows any material weaknesses in internal controls in year t (weak).

Preliminary Results

Table 2 reports the result of Hypothesis 1. Model (1)-(3) indicates that there is a significant positive association between competitive threats from the product market and data breaches. The results support Hypothesis 1. It indicates that competitive threats from the product market could increase the likelihood of a firm's data breaches. Using model (3) as an example, the coefficient of our independent variable ln_prodmktfluid is 0.466, which means the data breach risk will increase by 0.466 when there is a 1 unit increase of competitive threats from the product market. Besides, we could also find the size (ln_emp) and the performance of the firm (ln_leverage, ln_mkvalt, ln_at) could also increase the likelihood of data breach risk. It is consistent with prior literature (Higgs et al. 2016; Wang et al. 2013). And a firm with a CIO or CTO is more likely to have data breach risk although we have controlled the size, performance, and internal weakness found by audits. It is somewhat different from the prior study (Haislip et al. 2021). There are some possible explanations for this result: 1) a CIO/CTO without IT experience could not prevent data breach risk effectively, 2) the short tenure of the CIO/CTO, IT committee is ineffective, 3) symbolic adoption (compared to substantive adoption) could diminish the effectiveness of IT security investments on preventing data breach (Angst et al. 2017). Further study is required in the future.

Besides, we also categorize the data breach into two types according to the volume of data records: a data breach event will be labeled as a mild event when the lost data records are less than 1,000, otherwise, the data breach event will be labeled as a severe event. We run two zero-inflated Poisson regressions using categorized data. We could find there is a significant positive association (coefficient = 0.8, $p < 0.01$) between competitive threats from the product market and severe data breaches. There is no such association between competitive threats and the mild data breach.

	(1)	(2)	(3)	(4)	(5)
	Breach	Breach	Breach	Breach (Mild)	Breach (Severe)
ln_prodmktfluid	0.383**	0.354**	0.466***	0.266	0.8***
	(0.168)	(0.149)	(0.13)	(0.164)	(0.214)
ln_emp	0.595***	0.536***	0.527***	0.509***	0.569***
	(0.085)	(0.074)	(0.061)	(0.078)	(0.098)

ln_sale	0.003 (0.167)	-0.088 (0.142)	-0.091 (0.108)	-0.176 (0.14)	0.025 (0.17)
ln_leverage	0.989** (0.487)	0.935** (0.428)	1.04*** (0.385)	1.273*** (0.462)	0.636 (0.657)
ln_mkvalt	0.154* (0.08)	0.168** (0.072)	0.156** (0.061)	0.127* (0.076)	0.2** (0.1)
ln_at	0.229*** (0.082)	0.2*** (0.071)	0.208*** (0.058)	0.261*** (0.072)	0.129 (0.096)
ln_material_weak	-0.04 (0.417)	-0.029 (0.39)	0.006 (0.38)	0.404 (0.429)	-0.433 (1.679)
ln_count_weak	-0.005 (0.413)	-0.022 (0.392)	-0.094 (0.386)	-0.348 (0.473)	0.45 (0.697)
ln_xi	2.663 (14.955)	2.397 (14.081)	2.845 (11.282)	1.364 (13.916)	5.734 (21.619)
CIO_CTO	0.504***	0.491***	0.526***	0.482***	0.612***
	(0.148)	(0.135)	(0.117)	(0.147)	(0.193)
constant	-33.799 (122.822)	-29.575 (115.638)	-33.409 (92.651)	-20.558 (114.286)	-59.994 (177.544)
inflate: weak			18.072 (469919.23)	22.015 (8918197)	20.537 (16988.072)
inflate: constant			-29.032	-33.966	-20.571
			(469919.07)	(8918196.9)	(16988.071)
observations	36645	36645	36645	36645	36645

Table 2 Estimated Results

*Standard errors are in parenthesis, *** p<0.01, ** p<0.05, * p<0.1*

Robustness Check

We employ a propensity score matching approach method to reduce the selection bias problem (Juhee Kwon and Eric Johnson 2018). After matching, we use the Logit, Poisson, and Zero-Inflated model to re-run our regressions. All results are shown in Table 3. We could find the results are consistent with our main results in Table 2. That is, there is a significant positive association between competitive threats from the product market and data breaches. We could also find a significant positive association between the presence of CIO/CTO and the data breaches. Besides, competitive threats from the product market have significant increasing effect on severe data breach but have no significant effect on mild data breach.

	(6)	(7)	(8)	(9)	(10)

	Breach	Breach	Breach	Breach (Mild)	Breach (Severe)
ln_prodmktfluid	0.922***	0.238*	0.238*	0.074	0.508**
	(0.352)	(0.131)	(0.131)	(0.165)	(0.219)
ln_emp	0.888***	0.212***	0.212***	0.201***	0.252**
	(0.197)	(0.06)	(0.06)	(0.076)	(0.1)
ln_sale	-1.428***	-0.302**	-0.302**	-0.406***	-0.157
	(0.376)	(0.12)	(0.12)	(0.155)	(0.19)
ln_leverage	-0.824**	-0.216	-0.216	-0.138	-0.342
	(0.411)	(0.153)	(0.153)	(0.194)	(0.252)
ln_mkvalt	0.042	0.002	0.002	-0.024	0.031
	(0.161)	(0.062)	(0.062)	(0.077)	(0.106)
ln_at	-0.077	-0.006	-0.006	0.035	-0.066
	(0.163)	(0.062)	(0.062)	(0.077)	(0.105)
ln_material_weak	0.078	-0.041	-0.041	0.506	-1.067
	(1.249)	(.528)	(.528)	(0.628)	(1.369)
ln_count_weak	.346	0.101	0.101	-0.374	1.05
	(1.327)	(0.545)	(0.545)	(0.71)	(1.25)
ln_xi	0.679	0.227	0.227	-0.459	0.611
	(3.638)	(1.41)	(1.41)	(2.006)	(1.975)
CIO_CTO	0.809**	0.207*	0.207*	0.132	0.345*
	(0.328)	(0.12)	(0.12)	(0.152)	(0.197)
constant	2.823	-1.003	-1.003	5.7	-7.218
	(31.122)	(12.016)	(12.016)	(17.081)	(16.83)
inflate: weak			-.179	-.463	20.399
			(194392.65)	(45728.716)	(9566.537)
inflate: Constant			-25.967	-21.998	-21.548
			(34798.804)	(8073.231)	(9566.535)
observations	704	704	704	704	704

Table 3 Estimated Results After Matching

*Standard errors are in parenthesis, *** p<0.01, ** p<0.05, * p<0.1*

Potential Contribution & Future Work

Our study contributes to IS field in several ways. First, prior IS cybersecurity research focuses on the characteristics of the top management team, IT investment, and security-related policies. We are the first to build a link between competitive threats from the product market and a firm's data breach. Our work suggests that competitive pressure could increase the data breach risk of the firm. We also contribute to IT governance's impact on cybersecurity by examining the effect of the CIO/CTO. Our finding is very interesting that the presence of a CIO/CTO could not reduce the data breach risk. Instead, it could

strengthen the risk. One possible explanation is short tenure or non-IT expertise CIO/CTO could not help prevent a data breach. Besides, the symbolic adoption of IT would dimmish the effectiveness of data security investment (Angst et al. 2017). Instead, it could increase the data breach risk when the firm faces large competitive threats. Our study also provides some practical value to firm cybersecurity work. Such as the role and responsibility of the CIO/CTO should be taken seriously in data protection work.

We only show a preliminary result of our study. Further work is needed in the following days. First, we plan to examine the effect of competitive threats from the product market on different types of data breaches, such as external vs. internal, malicious vs. non-malicious, and financial vs. non-financial. Second, we also would like to further explore the reason for the increasing effect of the CIO/CTO. Third, some instrument variables are needed to support the causal inference. Fourth, we would like to find some alternative measurements of competitive threats for robustness checks.

Reference

Angst, C. M., Block, E. S., D'Arcy, J., and Kelley, K. 2017. "When Do It Security Investments Matter? Accounting for the Influence of Institutional Factors in the Context of Healthcare Data Breaches," MIS Quarterly (41:3), MIS Quarterly, pp. 893-A8.

Ashraf, M. 2022. "The Role of Peer Events in Corporate Governance: Evidence from Data Breaches," Accounting Review (97:2), American Accounting Association, pp. 1–24. (https://doi.org/10.2308/TAR-2019-1033).

Autor, D. H. 2003. "Outsourcing at Will: The Contribution of Unjust Dismissal Doctrine to the Growth of Employment Outsourcing," Journal of Labor Economics (21:1), pp. 1–42.

Barbos, A. 2015. "Information Acquisition and Innovation under Competitive Pressure," Journal of Economics & Management Strategy (24:2), pp. 325–347. (https://doi.org/10.1111/jems.12096).

Baumann, F., and Friehe, T. 2016. "Competitive Pressure and Corporate Crime," The B.E. Journal of Economic Analysis & Policy (16:2), De Gruyter, pp. 647–687. (https://doi.org/10.1515/bejeap-2015-0064).

Bisogni, F., and Asghari, H. 2020. "An Investigation into the Connection Between Data Breaches, Identity Theft, and Data Breach Notification Laws," Journal of Information Policy (10), University Pk: Penn State Univ Press, pp. 45–82. (https://doi.org/10.5325/jinfopoli.10.2020.0045).

Boubaker, S., Dang, V. A., and Sassi, S. 2022. "Competitive Pressure and Firm Investment Efficiency: Evidence from Corporate Employment Decisions," European Financial Management (28:1), pp. 113–161. (https://doi.org/10.1111/eufm.12335).

Chen, T., Kenneth Cheng, H., (Jimmy) Jin, Y., Li, S., and Qiu, L. 2021. "Impact of Competition on Innovations of IT Industry: An Empirical Investigation," Journal of Management Information Systems (38:3), pp. 647–666. (https://doi.org/10.1080/07421222.2021.1962590).

Cheng, L., Liu, F., and Yao, D. (Daphne). 2017. "Enterprise Data Breach: Causes, Challenges, Prevention, and Future Directions," WIREs Data Mining and Knowledge Discovery (7:5), p. e1211. (https://doi.org/10.1002/widm.1211).

D'Arcy, J., Adjerid, I., Angst, C. M., and Glavas, A. 2020. "Too Good to Be True: Firm Social Performance and the Risk of Data Breach," Information Systems Research (31:4), INFORMS, pp. 1200–1223. (https://doi.org/10.1287/isre.2020.0939).

Goode, S., Hoehle, H., Venkatesh, V., and Brown, S. A. 2017. "User Compensation as a Data Breach Recovery Action: An Investigation of the Sony Playstation Network Breach," MIS Quarterly (41:3), MIS Quarterly, pp. 703-A16.

Gwebu, K. L., Wang, J., and Wang, L. 2018. "The Role of Corporate Reputation and Crisis Response Strategies in Data Breach Management," Journal of Management Information Systems (35:2), Routledge, pp. 683–714. (https://doi.org/10.1080/07421222.2018.1451962).

Haislip, J., Lim, J.-H., and Pinsker, R. 2021. "The Impact of Executives' IT Expertise on Reported Data Security Breaches," Information Systems Research (32:2), INFORMS, pp. 318–334. (https://doi.org/10.1287/isre.2020.0986).

Higgs, J. L., Pinsker, R. E., Smith, T. J., and Young, G. R. 2016. "The Relationship between Board-Level Technology Committees and Reported Security Breaches," Journal of Information Systems (30:3), pp. 79–98. (https://doi.org/10.2308/isys-51402).

Hoberg, G., Phillips, G., and Prabhala, N. 2014. "Product Market Threats, Payouts, and Financial Flexibility," The Journal of Finance (69:1), pp. 293–324. (https://doi.org/10.1111/jofi.12050).

Hughes-Morgan, M., and Ferrier, W. J. 2017. "'Short Interest Pressure' and Competitive Behaviour," British Journal of Management (28:1), pp. 120–134. (https://doi.org/10.1111/1467-8551.12166).

Iriyama, A., Kishore, R., and Talukdar, D. 2016. "Playing Dirty or Building Capability? Corruption and HR Training as Competitive Actions to Threats from Informal and Foreign Firm Rivals," Strategic Management Journal (37:10), pp. 2152–2173. (https://doi.org/10.1002/smj.2447).

Janakiraman, R., Lim, J. H., and Rishika, R. 2018. "The Effect of a Data Breach Announcement on Customer Behavior: Evidence from a Multichannel Retailer," Journal of Marketing (82:2), American Marketing Association, pp. 85–105. (https://doi.org/10.1509/jm.16.0124).

Juhee Kwon, and Eric Johnson, M. 2018. "Meaningful Healthcare Security: Does Meaningful-Use Attestation Improve Information Security Performance?," MIS Quarterly (42:4), MIS Quarterly, pp. 1043–1067. (https://doi.org/10.25300/MISQ/2018/13580).

Kumari, A., Prakash, P., and Umadevi, M. 2021. "Prediction of Data Breaches Using Classification Algorithms," in Proceedings of the 2021 Fifth International Conference on I-Smac (Iot in Social, Mobile, Analytics and Cloud) (i-Smac 2021), New York: Ieee, pp. 1049–1054. (https://doi.org/10.1109/I-SMAC52330.2021.9640844).

Lending, C., Minnick, K., and Schorno, P. J. 2018. "Corporate Governance, Social Responsibility, and Data Breaches," Financial Review (53:2), pp. 413–455. (https://doi.org/10.1111/fire.12160).

Li, H., Yoo, S., and Kettinger, W. J. 2021. "The Roles of IT Strategies and Security Investments in Reducing Organizational Security Breaches," Journal of Management Information Systems (38:1), pp. 222–245. (https://doi.org/10.1080/07421222.2021.1870390).

Li, S., and Zhan, X. 2019. "Product Market Threats and Stock Crash Risk," Management Science (65:9), pp. 4011–4031. (https://doi.org/10.1287/mnsc.2017.3016).

Liu, C.-W., Huang, P., and Lucas, H. C. 2020. "Centralized IT Decision Making and Cybersecurity Breaches: Evidence from U.S. Higher Education Institutions," Journal of Management Information Systems (37:3), pp. 758–787. (https://doi.org/10.1080/07421222.2020.1790190).

McLeod, A., and Dolezel, D. 2018. "Cyber-Analytics: Modeling Factors Associated with Healthcare Data Breaches," Decision Support Systems (108), pp. 57–68. (https://doi.org/10.1016/j.dss.2018.02.007).

Min Wang and Zuosu Jiang. 2017. "The Defining Approaches and Practical Paradox of Sensitive Data: An Investigation of Data Protection Laws in 92 Countries and Regions and 200 Data Breaches in the World," International Journal of Communication (19328036) (11), University of Southern California, USC Annenberg Press, pp. 3286–3305.

Privacy Rights Clearinghouse. 2019. "What's a Data Breach?," , July 11. (https://privacyrights.org/resources/whats-data-breach, accessed April 29, 2022).

Rahulamathavan, Y., Rajarajan, M., Rana, O. F., Awan, M. S., Burnap, P., and Das, S. K. 2015. "Assessing Data Breach Risk in Cloud Systems," in 2015 Ieee 7th International Conference on Cloud Computing Technology and Science (Cloudcom), New York: Ieee, pp. 363–370. (https://doi.org/10.1109/CloudCom.2015.58).

Schwartz, P. M., and Janger, E. J. 2007. "Notification of Data Security Breaches," Michigan Law Review (105:5), Ann Arbor: Mich Law Rev Assoc, pp. 913–984.

Smith, T., Tadesse, A. F., and Vincent, N. E. 2021. "The Impact of CIO Characteristics on Data Breaches," International Journal of Accounting Information Systems (43), p. 100532. (https://doi.org/10.1016/j.accinf.2021.100532).

Wang, L., Jajodia, S., and Wijesekera, D. 2004. "Securing OLAP Data Cubes against Privacy Breaches," in 2004 Ieee Symposium on Security and Privacy, Proceedings, Los Alamitos: Ieee Computer Soc, pp. 161–175. (https://www.webofscience.com/wos/woscc/full-record/WOS:000222322800012).

Wang, T., Kannan, K. N., and Ulmer, J. R. 2013. "The Association Between the Disclosure and the Realization of Information Security Risk Factors," Information Systems Research (24:2), pp. 201–218. (https://doi.org/10.1287/isre.1120.0437).