Identifying Data Breaches Timely: Boards' Technology Committee Matters

Shan Xu
Xi'an Jiaotong University, sxu224-c@my.cityu.edu.hk

Ben Liu
City University of Hong Kong, ben.liu@cityu.edu.hk

Jin Li
School of Management, Xi'an Jiaotong University, jinlimis@xjtu.edu.cn

Identifying Data Breaches Timely: Boards' Technology Committee Matters

Short Paper

Shan Xu
Xi'an Jiaotong University
28 Xianning West Road, Beilin District, Xi'an, China.
City University of Hong Kong
Tat Chee Avenue, Kowloon, Hong Kong
sxu224-c@my.cityu.edu.hk

Ben Liu
City University of Hong Kong
Tat Chee Avenue, Kowloon, Hong Kong
ben.liu@cityu.edu.hk

Jin Li
Xi'an Jiaotong University
28 Xianning West Road, Beilin District, Xi'an, China.
jinlimis@xjtu.edu.cn

Abstract

This study investigates the effect of having a board-level technology committee on the time it takes for firms to identify a data breach. Data breach is one of the most important risks firms face. Boards of directors play a key role in overseeing these risks. The technology committee is an important means through which boards play this role. We present preliminary results using a sample of public firms that experienced data breaches between 2010 and 2021. Our results show that firms with technology committees can identify data breaches more quickly than those without. We also outline our future research agenda to address potential endogeneity issues and explore the underlying mechanisms. This study will contribute to the cybersecurity and corporate governance literature by demonstrating the effect of technology committees on firms' ability to identify data breaches.

Keywords: Data breach, Technology committee, Corporate governance, Identification time

Introduction

The board of directors has an important responsibility of monitoring potential risks, including those related to cybersecurity. The Securities and Exchange Commission (SEC) has proposed that firms disclose how the board monitors the management of cybersecurity risks (SEC 2018). However, many boards are unprepared and lack awareness in effectively monitoring cybersecurity risks (Rothrock et al., 2018). According to the Identity Theft Resource Center (ITRC), there were 1,802 data breaches in 2022, just 60 events shy of the previous record. The average costs of data breaches reached an all-time high of USD 4.35 million in 2022, a 2.6% increase from the previous year. These statistics indicate ongoing threats to firms' cybersecurity and suggest that boards may not be adequately monitoring or supporting management in reducing these risks.

The board of directors plays a crucial role in shaping a firm's strategy and investment decisions regarding data breach prevention, reporting, and control (Higgs et al., 2016). While the IT security team is responsible for implementing and maintaining security systems and policies, the ultimate accountability for data breaches should not solely be placed on the IT department. It is not uncommon for firms to invest heavily in IT security systems yet still experience data breaches due to human negligence or errors. Target's data breach incident serves as an example, where despite having an advanced cybersecurity system in place, the breach went unnoticed due to ignored warning messages and disabled malware eradication functions

(Smith, 2014). This highlights a lack of proper supervision and control over unsafe actions that facilitated the breach. If Target had exercised more vigilance and oversight over cybersecurity issues and closely monitored the actions of IT executives and staff, the breach could have been identified earlier (Hoehle et al., 2022; Smith, 2014).

Prior studies examine various factors that influence the likelihood and severity of data breaches, as well as the response strategies that mitigate the associated costs. During such data security crises, affected firms face mounting pressure from stakeholders and the media to respond promptly (Hegner et al., 2016). However, there is a dearth of studies focusing on the time it takes for firms to identify data breaches, which is the time elapsed from the occurrence to the detection of a cyberattack. Nikkhah and Grover (2022) conclude that timely announcement after a data breach is crucial and can affect customer and investor behaviors through response strategies. An extended identification time may allow the attackers to access a larger amount of data, leading to more substantial financial and non-financial consequences. Supporting this notion, a report by IBM in 2022 reveals that the average time it takes to identify a data breach is 207 days, and the average time to contain it is 70 days (IBM Security, 2022). Furthermore, breaches with durations shorter than 200 days result in an average cost saving of USD 1.12 million compared to those lasting longer than 200 days. This finding underscores the significant impact of reducing the time required for breach identification and containment. Considering that the average cost of a data breach stands at roughly USD 4.35 million, the potential savings associated with a shorter breach identification time are substantial. Therefore, the primary focus of this study is to investigate timely breach identification in order to assist organizations in minimizing the costs associated with data breaches.

A technology committee is a specialized board-level committee that oversees technology-related issues, including cybersecurity (Higgs et al., 2016). This committee's presence may impact a firm's cybersecurity strategy and practices. Our study investigates whether technology committees enable firms to detect data breaches more quickly. We collect and analyze data from multiple sources to answer this question. Preliminary results suggest that having a technology committee is associated with a shorter data breach identification time. This study contributes to the data breach literature by examining the impact of technology committees on firms' data breach identification time, which can significantly affect data breach outcomes. Additionally, our study will explore the mechanisms through which technology committees facilitate faster identification of data breaches. Furthermore, we will examine how data breach identification time affects the cost of data breaches, providing empirical evidence for the negative consequences of a prolonged identification time and the potential cost savings associated with faster identification.

Related Literature

Antecedents of Data Breaches

The adoption of information technologies can threaten organizations' data security. In the healthcare industry, hospitals have implemented electronic health records systems (EHRs) and pursued meaningful use (MU) attestation. MU attestation may result in more internal data breaches in the short term (Kwon & Johnson, 2018). Implementing EHRs can increase the likelihood of patient data breach and accidental data breach (Kim and Kwon, 2019). To address these risks, investing in IT security measures is necessary. In the healthcare industry, proactive investments made before a data breach can reduce breach rates and are more effective than reactive investments (Kwon & Johnson, 2018). The impact of IT security investments may vary across organizations. In highly digitalized organizations, such investments may increase the risk of data breaches, while in less digitalized organizations, they may decrease the risk (Li et al., 2021). IT security investments can also have spillover effects, benefiting both the investing firm and its competitors, ultimately improving industry-wide security (Jeong et al., 2019). However, contrasting findings suggest that increased IT security expenditures may actually heighten the risk of data breaches (Sen and Borle 2015).

Given that investing in IT security is not a foolproof solution to preventing data breaches, a number of studies also examine the effect of management-level factors on data breach incidents. After a data breach, executives may face penalties or termination, which encourages them to prioritize data breach prevention (Schlackl et al., 2022). The Chief Information Officer (CIO), as a vital member of the top management team (TMT), plays a key role in addressing emerging cybersecurity risks (Feng & Wang, 2019). A risk-averse CIO with greater power is associated with a lower likelihood of breaches (Feng & Wang, 2019). However, the

responsibility for information security extends beyond CIO, and the TMT must collaborate to enhance IT governance (Haislip et al., 2021). TMT members with expertise in IT contribute to reducing the likelihood of data breaches, highlighting the importance of TMT effort (Haislip et al., 2021).

Several studies investigate the relationship between board-level characteristics and data breaches. One important characteristic that can influence boards' ability to address cybersecurity issues is the IT expertise of board members. It is crucial for board members to possess IT expertise in order to understand the actions of CIOs and the IT department, enabling them to effectively monitor their activities. Having IT experts on boards can also offer advisory roles, which can help mitigate potential cybersecurity risks (Chen et al., 2022). Additionally, the characteristics of a CEO can also impact the effectiveness of board monitoring. CEO power is one such characteristic that can affect board monitoring beyond its effect on the selection and appointment of directors (Lisic et al., 2016).

Response Strategies to Data Breaches

One challenge that firms face after a data breach is how to minimize its impact on their reputation and performance. Firms have discretion in deciding when to disclose a data breach, as U.S. states have laws requiring disclosure but without a specific deadline (Foerderer & Schuetz, 2022). According to Foerderer and Schuetz (2022), firms can manipulate stock market outcomes by strategically timing data breach disclosures. They tend to disclose breaches on days with higher news pressure to reduce media and investor attention, thus mitigating negative stock market reactions.

Firms can address the consequences of a data breach by apologizing, compensating, or justifying their actions to the affected parties, such as customers and shareholders. However, the effects of these strategies can vary among different stakeholders. Apologizing for a data breach has negative effects on investor behaviors but positive effects on consumer behaviors (Masuch et al., 2019, 2021). This suggests that investors may interpret an apology as an admission of guilt, but consumers may appreciate the sincerity of the firm. The impact of compensation can also differ significantly. Compensation can influence consumers' perceptions of justice, which in turn affects their satisfaction and loyalty levels (Goode et al. 2017). To achieve favorable customer outcomes, firms should align their compensation efforts with customers' expectations (Hoehle et al., 2022). Justifying firms' actions does not significantly affect investor behaviors (Masuch et al., 2022). The effectiveness of these strategies may also depend on the firms' prior reputations. These strategies have limited effects on firms with high reputation, but they may help mitigate adverse financial effects for firms with relatively low reputation (Gwebu et al., 2018).

The existing literature extensively examines the factors that contribute to the occurrence of data breaches in the pre-breach phase, as well as the response strategies employed to mitigate associated costs once a data breach incident is identified. However, there is a significant gap in the literature regarding the crucial event that takes place between the occurrence of the breach and the initiation of a response. In order to address this gap, our study seeks to specifically examine the time it takes to identify data breaches. By doing so, our study can bridge the divide between studies that primarily focus on the pre-breach phase and those that concentrate on the post-identification phase of data breaches. It is important to note that the identification time can vary significantly among firms that have experienced data breaches, and is often quite lengthy (IBM Security, 2022). In light of this, reducing the identification time is crucially important, as faster detection can help mitigate the severity and cost of a data breach. Against this background, our study examines the time difference between the occurrence and the detection of data breaches, with the aim of aiding in the reduction of the identification time.

Theoretical Development: Technology Committee and Data Breach Identification Time

As per the upper echelon theory, the board of directors assumes a crucial role in shaping a firm's decision-making process and influencing its outcomes (Hambrick & Mason, 1984; Terbeck et al., 2022). Therefore, we argue that the characteristics of the board can have an impact on a firm's decisions concerning cybersecurity, which in turn can affect the time taken to detect data breaches. Following the occurrence of a data breach, firms often take measures to enhance their IT governance at the board level (Benaroch & Chernobai, 2017). One way to achieve this objective is to establish a technology committee that offers guidance and support to the management on IT-related matters (Benaroch & Chernobai, 2017; Price &

Lankton, 2018). Following this logic, we focus on a specific characteristic of the board, that is, whether it has a technology committee. It is worth noting that many firms create technology committees and appoint IT experts to assist the boards in overseeing IT and cybersecurity risks (Hartmann & Carmenate, 2021). Technology committees are board-level committees that are responsible for overseeing and advising on IT and other technology-related issues (Premuroso & Bhattacharya, 2007). The number of technology committees among public companies has been growing steadily over the years and around 12% of Global Fortune 500 companies had standing technology committees in 2022 (Hartmann & Carmenate, 2021; McKinsey, 2022). Moreover, technology committees are more common in industries that depend more on information technologies, such as telecom and healthcare, where ITs are vital for the firm's competitive advantage and value creation (McKinsey, 2022).

Technology committees may help reduce data breach identification time in several ways. First, through the establishment of a technology committee, a board can effectively convey to shareholders its commitment to IT-related matters (Higgs et al., 2016). This strategic move demonstrates the board's recognition of IT risks. The active and supportive engagement of boards in cybersecurity issues may foster a culture whereby cybersecurity is viewed as a standard practice rather than an exception (Johnston & Hale, 2009; Schinagl & Shahim, 2020). By fostering such a culture, the firm's awareness and preparedness for cyber threats can be strengthened, and the identification time of data breaches may be reduced. Second, technology committees can help detect data breaches more effectively by setting up processes and controls that IT executives can follow. Boards have a responsibility to provide guidance on firms' IT processes (Haislip et al., 2020). To enhance the effectiveness of this responsibility, a board can assign some cybersecurity-related tasks to the technology committee (Premuroso & Bhattacharya, 2007). Technology committees outline proper IT processes and controls (Haislip et al., 2020). IT executives can then implement these processes and controls to manage cybersecurity risks and ensure the firm's timely identification of data breaches. Due to the above two reasons, we expect that having a technology committee is associated with reduced data breach identification time.

Preliminary Analysis

Sample and Variables

We collect data from three sources, including the Audit Analytics, Compustat, and BoardEx. We obtain data breach records for public firms from Audit Analytics. After excluding the missing values (i.e., data breach records that do not have the date of data breach occurrence or time it takes to identify the data breach), we obtain 329 data breach records between 2010 and 2021. We then collect information on firms' board-level committees and employment experiences of board members and CEOs for public firms that experienced data breaches during the sampling period from BoardEx. Additionally, we gather financial information, geographic location, and industry related information for firms in our sample from the Compustat database. We match firms across the three data sources using the CUSIP number. The final sample contains 213 data breach records with relevant firm and board characteristics.

The dependent variable in our study is data breach identification time, which captures how quickly a firm can detect a data breach event (IBM Security, 2022). We measure this variable through the number of days between the breach occurrence and the event detection. We take the natural logarithm due to its skewed distribution and high variance. The average time to identify data breaches involving different types of information vary significantly. It takes 86 days to identify data breaches that exposed personal information, while data breaches that compromised financial information take almost twice as long, with an average of 164 days.

Following Higgs et al. (2016), we create a binary variable to capture whether a firm has a technology committee. This binary variable takes the value of 1 if the firm has a technology committee at the time of the data breach, and 0 otherwise. In our sample, approximately 10.8% of the firms have a technology committee. It is possible that firms may create other board-level committees to oversee data breach risks, such as risk or compliance committees. Therefore, we control for the presence of these two types of committees in our model. We similarly create two binary variables to measure the presence of these two committees (Higgs et al., 2016). Firms may delegate the task of monitoring cybersecurity risks to their audit committees (Ashraf et al., 2020). In order to account for this possibility, we manually gather the proxy statements of the firms in our final sample and carefully identify the specific responsibilities assigned to the

audit committees. To measure whether an audit committee is tasked with this responsibility, we create a binary variable, "$ACCyberRisk$", which takes a value of 1 if the audit committee is responsible for monitoring cybersecurity risk and 0 otherwise.

We also control for CEO power because it may affect the decision to form a technology committee and the effectiveness of board monitoring. Following prior research (Fracassi & Tate, 2012), we measure CEO power based on CEO tenure and whether a CEO also takes the chairman or president role in the firm. We measure CEO tenure through the number of years that the CEO has been in office. We create a binary variable to indicate whether a CEO take multiple roles. The variable equals 1 if a CEO is also the chairman or president, and 0 otherwise. Because high-tech firms are more likely to use information technologies and have greater expertise to deal with cyber-attacks (Haislip et al., 2021), we also create a binary variable to control for high-tech firms. The variable equals 1 if a firm belongs to the high-tech industry based on the Standard Industrial Classification (SIC) code and 0 otherwise. Since firm characteristics may influence the choice of forming a technology committee and the ability to identify data breaches, we control for firm size, financial leverage, whether the firm is loss-making, return on assets (ROA), and whether the firm has engaged in mergers and acquisitions (Haislip et al., 2021; Higgs et al., 2016). We measure firm size through the natural logarithm of the firm's total assets and financial leverage through the ratio of total liabilities to total assets. We create a binary variable to indicate whether the firm has reported a net loss (Haislip et al., 2021; Higgs et al., 2016). We calculate ROA by dividing net income by total assets. We create another binary variable to indicate whether the firm has engaged in mergers and acquisitions (Haislip et al., 2021). We also include board size as a control variable, as larger boards may have more resources to deal with cybersecurity issues (Chen et al., 2022). Board size is measured through the number of directors on board (Chen et al., 2022). Following Ashraf et al. (2020), we control for the existence of IT experts on board. We measure IT expertise based on board members who have held IT executive positions including CIO, director of IT, and head or manager of Information Services, Information Technology, Information Management, or Information Systems.

Preliminary Results

We run the following OLS regression to investigate the effect of technology committees on data breach identification time:

$$Ln\left(IdentificationTime_{ijt}\right) = \beta \times TechCommittee_{it} + Controls_{it} + \theta_i + \lambda_t + \varepsilon_{ijt}$$

where $IdentificationTime_{ijt}$ is jth data breach of firm i in year t. $Controls_{it}$ includes the control variables described above. We include industry fixed effects using the 2-digit SIC code and year fixed effects (represented by θ_i and λ_t, respectively). ε_{ijt} is the error term. Standard errors are clustered at firm level.

Table 1 reports the OLS regression results. We progressively add the controls to the model. Column (1) includes other board-level committees which may also be responsible for IT-related issues. We additionally include CEO characteristics and high-tech industry controls in columns (2) and (3) respectively. All columns include the control variables that capture firm-specific and board-level characteristics. We explain our findings based on the results in column (3). There is a statistically significant and negative relationship between the presence of a technology committee and data breach identification time (β=-0.9828, p-value=0.054). The results show that firms with a technology committee are associated with a 98.28% decrease in data breach identification time. However, the estimated effects of $RiskCommittee$ and $ComplianceCommittee$ are indistinguishable from zero (p-value=0.525 and 0.111, respectively). This may suggest that technology committees have a more direct and specific role in overseeing and advising on IT and data security issues, but risk and compliance committees may have broader and more general responsibilities that may not directly impact data breach identification time. Moreover, the coefficient of $ACCyberRisk$ is insignificant (p-value=0.503). This could be attributed to the fact that audit committees have numerous responsibilities, and the cybersecurity may not always be their top priority. The coefficient of $TechCommittee$ remains stable when we control for CEO characteristics and whether the firm is in high-tech industry. This suggests that link between technology committees and data breach identification time is not confounded by CEO characteristics or whether the firm is in the high-tech industry.

	(1)	(2)	(3)
TechCommittee	-0.8948*	-0.9008*	-0.9828*

	(0.5229)	(0.5307)	(0.5061)
RiskCommittee	0.2748	0.3166	0.2714
	(0.4227)	(0.4366)	(0.4258)
ComplianceCommittee	0.6585	0.7205	0.7148
	(0.4377)	(0.4519)	(0.4464)
ACCyberRisk	0.1509	0.3179	0.2860
	(0.4112)	(0.4274)	(0.4263)
CEOMultipleRoles		0.5774	0.5951
		(0.3676)	(0.3649)
CEOTenure		0.0099	0.0120
		(0.0253)	(0.0247)
HighTech			-0.8274
			(0.5149)
FirmSize	-0.1991**	-0.1747*	-0.1624
	(0.0986)	(0.1022)	(0.1048)
Leverage	-0.3518	-0.3361	-0.4966
	(0.7166)	(0.6983)	(0.7136)
Loss	0.4355	0.4858	0.5571
	(0.4580)	(0.4739)	(0.4617)
ROA	-1.2045	-1.1785	-1.3998
	(1.0214)	(1.0765)	(1.0716)
Merger	-0.1446	-0.2350	-0.2397
	(0.3950)	(0.3935)	(0.3957)
BoardSize	0.1125	0.1010	0.1013
	(0.0793)	(0.0793)	(0.0803)
ITExpert	0.2832	0.2823	0.4272
	(0.3229)	(0.3245)	(0.3286)
Industry fixed effects	Included	Included	Included
Year fixed effects	Included	Included	Included
R^2	0.297	0.310	0.320
Observations	213	213	213

Notes: * p< 0.1; ** p< 0.05; *** p< 0.01. Standard errors are in parentheses. Standard errors are robust and clustered at firm level. The dependent variable is the natural log of the identification time of a data breach.

Table 1. OLS Regression Results

Future Research Steps

To move forward and complete this study, we will perform several further steps. First, we will manually collect and verify the data on the occurrence and identification dates of data breaches for the public firms in our sample, as some of these data are missing or incomplete in the dataset we use. We will also manually match the firms across the three datasets to increase our sample size. Second, we will address the potential endogeneity issue in our research. The link between technology committees and data breach identification

time may not have a causal interpretation due to the presence of confounding omitted variables. For instance, firms that prioritize cybersecurity may be more likely to form a technology committee and at the same time identify data breaches sooner. We plan to use an instrumental variable strategy to address the omitted variable issue. One possible instrument is the average rate of technology committees within the same city and industry as the focal firm. This instrumental variable aims to capture peer effects on the establishment of a technology committee, which are not directly linked to the time it takes to identify a data breach. Third, we will examine the possible mechanisms through which the technology committee affects firm' s capability to identify a data breach. One possible mechanism is that the technology committee may foster a cybersecurity-focused culture, leading to a shorter identification time of data breach. By promoting a culture of cybersecurity, the technology committee is expected to enhance the firm's internal control over IT. Hence, one way to probe this mechanism is to investigate whether the presence of a technology committee strengthens the firm's internal control over IT. To measure the level of internal control in relation to IT, we plan to use the number of material weaknesses associated with IT as a proxy. The second underlying mechanism is that the technology committee may provide valuable guidance to executives by outlining suitable IT processes and controls, resulting in better management of cybersecurity issues. To examine this mechanism, we will use data on executives' IT-related experience and educational background as proxies for their guidance needs. We expect that the impact of the technology committee will be more pronounced in firms where executives require cybersecurity guidance compared to firms where there is less demand for such guidance. Finally, we will quantify the effect of data breach identification time on the costs of data breaches. To achieve this, we propose to use the economic impacts of data breaches as a measure of their costs. Specifically, we will adopt the approach introduced by Benaroch and Chernobai (2017), which involves assessing cumulative abnormal stock returns. This measure is calculated by summing the differences between the actual daily stock returns and the expected returns within a 3-day event period. Although there exists some anecdotal evidence suggesting a relationship between the time taken to identify a data breach and its costs, the magnitude of this effect remains unclear. Our research seeks to employ regression analyses to quantitatively assess this relationship. By doing so, we aim to provide insights that can have significant implications for both firms and policymakers.

Limitations

This study has some limitations. First, our results may suffer from measure errors because the reported data breach dates might not be accurate. We will validate our data based on data from Privacy Rights Clearinghouse (PRC), which provides a description for each data breach. Second, the small sample size might be a concern in this preliminary analysis. We will increase our sample size by gathering data from other data breach chronology platforms such as PRC. Third, we use a binary variable to indicate whether the firm has a board-level technology committee. This indicator does not capture committee member diversity or quality of the committee. Future research may overcome these limitations by using more granular and valid data sources and measures.

Intended Contributions

This study seeks to contribute to the existing literature on corporate governance and data breach management. First, while prior research primarily focuses on the antecedents and response strategies to data breaches, little attention has been given to data breach identification time. Recent evidence shows that firms take a considerable amount of time to identify data breaches, and there is a substantial variation in identification time across different organizations. Additionally, longer identification times are typically associated with higher costs incurred due to data breaches. In order to address this research gap, our study will investigate the potential role of technology committees in reducing data breach identification time. Furthermore, we will explore the link between identification time and the costs associated with data breaches. Second, we will explore the underlying mechanisms driving the effect of technology committees on data breach identification time. By doing so, we seek to enhance our understanding of the factors that contribute to timely identification of data breaches. Our theoretical framework posits that technology committees play a crucial role in reducing identification time by improving firms' internal control mechanisms and providing valuable guidance for executives. These mechanisms will be empirically tested in our future research. Lastly, our study will examine the relationship between data breach identification time and costs. By presenting evidence confirming the negative link between these variables, we will

demonstrate the potential benefits of swift data breach identification. Our results will provide a clearer understanding of the importance of shortening data breach identification time, as well as the merits of establishing a technology committee.

References

Ashraf, M., Michas, P. N., & Russomanno, D. (2020). The Impact of Audit Committee Information Technology Expertise on the Reliability and Timeliness of Financial Reporting. *The Accounting Review*, *95*(5), 23–56. **https://doi.org/10.2308/accr-52622**

Benaroch, M., & Chernobai, A. (2017). Operational It Failures, It Value Destruction, and Board-Level It Governance Changes. *MIS Quarterly*, *41*(3), 729-762. **https://doi.org/10.25300/MISQ/2017/41.3.04**

Chen, C., Hartmann, C., & Gottfried, A. (2022). The Impact of Audit Committee IT Expertise on Data Breaches. *Journal of Information Systems*, *36*(3), 61–81. **https://doi.org/10.2308/ISYS-2020-076**

Feng, C. (Qian), & Wang, T. (2019). Does CIO risk appetite matter? Evidence from information security breach incidents. *International Journal of Accounting Information Systems*, *32*, 59–75. **https://doi.org/10.1016/j.accinf.2018.11.001**

Foerderer, J., & Schuetz, S. W. (2022). Data Breach Announcements and Stock Market Reactions: A Matter of Timing? *Management Science*. **https://doi.org/10.1287/mnsc.2021.4264**

Fracassi, C., & Tate, G. (2012). External Networking and Internal Firm Governance. *The Journal of Finance*, *67*(1), 153–194. **https://doi.org/10.1111/j.1540-6261.2011.01706.x**

Goode, S., Hoehle, H., Venkatesh, V., & Brown, S. A. (2017). User compensation as a data breach recovery action: An investigation of the sony PlayStation network breach. *MIS Quarterly*, *41*(3), 703–727. **https://doi.org/10.25300/MISQ/2017/41.3.03**

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

Haislip, J., Lim, J.-H., & Pinsker, R. (2021). The impact of executives' IT expertise on reported data security breaches. *Information Systems Research*, *32*(2), 318–334. **https://doi.org/10.1287/isre.2020.0986**

Haislip, J. Z., Karim, K. E., Lin, K. J., & Pinsker, R. E. (2020). The Influences of CEO IT Expertise and Board-Level Technology Committees on Form 8-K Disclosure Timeliness. *Journal of Information Systems*, *34*(2), 167–185. **https://doi.org/10.2308/isys-52530**

Hambrick, D. C., & Mason, P. A. (1984). Upper Echelons: The Organization as a Reflection of Its Top Managers. *The Academy of Management Review*, 9(2), 193–206.

Hartmann, C. C., & Carmenate, J. (2021). Academic Research on the Role of Corporate Governance and IT Expertise in Addressing Cybersecurity Breaches: Implications for Practice, Policy, and Research. *Current Issues in Auditing*, *15*(2), A9–A23. **https://doi.org/10.2308/CIIA-2020-034**

Hegner, S. M., Beldad, A. D., & Kraesgenberg, A.-L. (2016). The Impact of Crisis Response Strategy, Crisis Type, and Corporate Social Responsibility on Post-crisis Consumer Trust and Purchase Intention. *Corporate Reputation Review*, 19(4), 357–370. **https://doi.org/10.1057/s41299-016-0007-y**

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. **https://doi.org/10.2308/isys-51402**

Hoehle, H., Venkatesh, V., Brown, S. A., Tepper, B. J., & Kude, T. (2022). Impact of Customer Compensation Strategies on Outcomes and the Mediating Role of Justice Perceptions: A Longitudinal Study of Target's Data Breach. *MIS Quarterly*, *46*(1), 299–340. **https://doi.org/10.25300/MISQ/2022/14740**

IBM Security. (2022, July 27). Cost of a data breach report 2022. https://www.ibm.com/security/digital-assets/cost-data-breach-report/

ITRC. (2023, January 25). 2022 data breach report. https://www.idtheftcenter.org/publication/2022-data-breach-report/

Jeong, C. Y., Lee, S.-Y. T., & Lim, J.-H. (2019). Information security breaches and IT security investments: Impacts on competitors. *Information & Management*, *56*(5), 681–695. **https://doi.org/10.1016/j.im.2018.11.003**

Johnston, A. C., & Hale, R. (2009). Improved Security through Information Security Governance. *Communications of the ACM*, *52*(1), 126–129. **https://doi.org/10.1145/1435417.1435446**

Kim, S. H., & Kwon, J. (2019). How Do EHRs and a Meaningful Use Initiative Affect Breaches of Patient Information? *Information Systems Research*, *30*(4), 1184–1202. **https://doi.org/10.1287/isre.2019.0858**

Kwon, J., & Johnson, M. E. (2018). Meaningful Healthcare Security: Does Meaningful-Use Attestation Improve Information Security Performance? *MIS Quarterly*, *42*(4), 1043–1067. **https://doi.org/10.25300/MISQ/2018/13580**

Kwon, J., & Johnson, M. E. (2014). Proactive Versus Reactive Security Investments in the Healthcare Sector. *MIS Quarterly*, *38*(2), 451-471. **https://doi.org/10.25300/MISQ/2014/38.2.06**

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

Lisic, L. L., Neal, T. L., Zhang, I. X., & Zhang, Y. (2016). CEO Power, Internal Control Quality, and Audit Committee Effectiveness in Substance Versus in Form. *Contemporary Accounting Research*, *33*(3), 1199–1237. **https://doi.org/10.1111/1911-3846.12177**

Masuch, K., Greve, M., & Trang, S. (2019). Does it meet my expectations? Compensation and remorse as data breach recovery actions – An experimental scenario based investigation. *WISP 2019 Proceedings*. **https://aisel.aisnet.org/wisp2019/13**

Masuch, K., Greve, M., & Trang, S. (2021). What to do after a data breach? Examining apology and compensation as response strategies for health service providers. *Electronic Markets*, *31*(4), 829–848. **https://doi.org/10.1007/s12525-021-00490-3**

Masuch, K., Greve, M., Trang, S., & Kolbe, L. M. (2022). Apologize or justify? Examining the impact of data breach response actions on stock value of affected companies? *Computers & Security*, *112*, 102502. **https://doi.org/10.1016/j.cose.2021.102502**

McKinsey. (2022, September 15). *How effective boards approach tech governance*. https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/how-effective-boards-approach-technology-governance

Nikkhah, H. R., & Grover, V. (2022). An Empirical Investigation of Company Response to Data Breaches. *MIS Quarterly*, 46(4), 2163–2196. **https://doi.org/10.25300/MISQ/2022/16609**

Premuroso, R. F., & Bhattacharya, S. (2007). Is There a Relationship between Firm Performance, Corporate Governance, and a Firm's Decision to Form a Technology Committee? *Corporate Governance: An International Review*, *15*(6), 1260–1276. **https://doi.org/10.1111/j.1467-8683.2007.00645.x**

Price, J. B., & Lankton, N. (2018). A Framework and Guidelines for Assessing and Developing Board-Level Information Technology Committee Charters. *Journal of Information Systems*, 32(1), 109–129. **https://doi.org/10.2308/isys-51674**

Rothrock, R. A., Kaplan, J., & Van Der Oord, F. (2018). The Board's Role in Managing Cybersecurity Risks. *MIT Sloan Management Review*, *59*(2), 12–15.

Schinagl, S., & Shahim, A. (2020). What do we know about information security governance? "From the basement to the boardroom": towards digital security governance. *Information & Computer Security*, *28*(2), 261–292. **https://doi.org/10.1108/ICS-02-2019-0033**

Schlackl, F., Link, N., & Hoehle, H. (2022). Antecedents and consequences of data breaches: A systematic review. *Information & Management*, *59*(4), 103638. **https://doi.org/10.1016/j.im.2022.103638**

SEC. (2018, February 26). *Commission Statement and Guidance on Public Company Cybersecurity Disclosures*. https://www.federalregister.gov/documents/2018/02/26/2018-03858/commission-statement-and-guidance-on-public-company-cybersecurity-disclosures

Sen, R., & Borle, S. (2015). Estimating the Contextual Risk of Data Breach: An Empirical Approach. *Journal of Management Information Systems*, *32*(2), 314–341. **https://doi.org/10.1080/07421222.2015.1063315**

Smith, C. (2014, March 14). It turns out Target could have easily prevented its massive security breach. BGR. https://bgr.com/general/target-data-hack-how-it-happened/

Terbeck, H., Rieger, V., Van Quaquebeke, N., & Engelen, A. (2022). Once a Founder, Always a Founder? The Role of External Former Founders in Corporate Boards. *Journal of Management Studies*, 59(5), 1284–1314. **https://doi.org/10.1111/joms.12774**